[1] C. Alcaraz and J. Lopez. WASAM: a dynamic wide-area situational awareness model for critical domains in smart grids. *Future Generation Computer Systems*, 30:146-154, Jan. 2014. [bib | DOI]

> Control from anywhere and at anytime is nowadays a matter of paramount importance in critical systems. This is the case of the Smart Grid and its domains which should be monitored through intelligent and dynamic mechanisms able to anticipate, detect and respond before disruptions arise within the system. Given this fact and its importance for social welfare and the economy, a model for wide-area situational awareness is proposed in this paper. The model is based on a set of current technologies such as the wireless sensor networks, the ISA100.11a standard and cloud-computing together with a set of high-level functional services. These services include global and local support for prevention through a simple forecast scheme, detection of anomalies in the observation tasks, response to incidents, tests of accuracy and maintenance, as well as recovery of states and control in crisis situations.

[2] C. Alcaraz and M. Sönmez Turan. PDR: A prevention, detection and response mechanism for anomalies in energy control systems. In B. M. Hämmerli, N. Kalstad Svendsen, and J. Lopez, editors, *Critical Information Infrastructures Security*, volume 7722 of *Lecture Notes in Computer Science*, pages 22-33. Springer Berlin Heidelberg, 2013. [bib | DOI]

> Prevention, detection and response are nowadays considered to be three priority topics for protecting critical infrastructures, such as energy control systems. Despite attempts to address these current issues, there is still a particular lack of investigation in these areas, and in particular in dynamic and automatic proactive solutions. In this paper we propose a mechanism, which is called PDR, with the capability of anticipating anomalies, detecting anomalous behaviours and responding to them in a timely manner. PDR is based on a conglomeration of technologies and on a set of essential components with the purpose of offering situational awareness irrespective of where the system is located. In addition, the mechanism can also compute its functional capacities by evaluating its efficacy and precision in the prediction and detection of disturbances. With this, the entire system is able to know the real reliability of its services and its activity in remote substations at all times.
>
> Keywords: Detection; Energy Control Systems; Industrial Wireless Sensor Networks; MANET; Prevention; Response; The Internet; and Wide-Area Situational Awareness

[3] B.-C. Bösch. Economical benefits of standardized intrusion detection parametrization. *International Journal of Scientific & Technology Research*, 1(10):18-23, Nov. 2012. [bib | .pdf]

> Intrusion Detection Systems (IDS) are very important to protect important services against malicious actions. Detailed knowledge of information processing and protocols are necessary to protect the services and systems sufficient against attacks. IDS are currently independent and coexisting solutions. Each single IDS requires its individual administration access, administration handling and management infrastructure. Possible savings of a standardized parameterization infrastructure over all IDS will be analyzed. In every part of the solution life cycle process, design, infrastructure and additional expenses were analyzed. Based on the Return-on-Security-Investments model the benefit of a standardized parameterization was pointed out.
>
> Keywords: IDPEF,IDXP,Intrusion Detection,Network Management,System Management

[4] B.-C. Bösch. Standardized parameterization of intrusion detection systems. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, 1(3):1-5, May 2012. [bib | .pdf]

[5] B.-C. Bösch. Approach to enhance the efficiency of security operation centers to heterogeneous ids landscapes. In B. M. Hämmerli, N. Kalstad Svendsen, and J. Lopez, editors, *Critical Information Infrastructures Security*, volume 7722 of *Lecture Notes in Computer Science*, pages 1-9. Springer Berlin Heidelberg, 2013. [bib | DOI]

> Critical infrastructures include large scale environments with different platforms and / or platform generations. The maintenance interval of such large scaled, distributed systems to patch

vulnerabilities increases with the amount of entities. IDS are necessary to protect the vulnerable system / entity until the patch will be applied to the distributed entity. This paper presents an approach to separate the IDS manager from the rest of an IDS by a standardized IDS parameterization independent of its scope (host based or network based IDS) and vendor. The exchange of the parameterization was integrated via communication modules in three open source IDS to demonstrate the common applicability of the format. An enhanced IDS model of the IETF will be illustrated.

Keywords: IDXP; Intrusion Detection; Standardization; Parameterization; IDS Management

[6] About common event expression - archive. http://cee.mitre.org/about/, retrieved Mar 4, 2014. [bib]

[7] L. Coppolino, S. D'Antonio, V. Formicola, and L. Romano. Integration of a system for critical infrastructure protection with the OSSIM SIEM platform: A dam case study. In F. Flammini, S. Bologna, and V. Vittorini, editors, *Computer Safety, Reliability, and Security*, volume 6894 of *Lecture Notes in Computer Science*, pages 199-212. Springer Berlin Heidelberg, 2011. [bib | DOI]

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

[8] L. Coppolino, S. D'Antonio, V. Formicola, and L. Romano. Enhancing SIEM technology to protect critical infrastructures. In B. M. Hämmerli, N. Kalstad Svendsen, and J. Lopez, editors, *Critical Information Infrastructures Security*, volume 7722 of *Lecture Notes in Computer Science*, pages 10-21. Springer Berlin Heidelberg, 2013. [bib | DOI]

Coordinated and targeted cyber-attacks on Critical Infrastructures (CIs) and Supervisory Control And Data Acquisition (SCADA) systems are increasing and becoming more sophisticated. Typically, SCADA has been designed without having security in mind, which is indeed approached by reusing solutions to protect solely Information Technology (IT) based infrastructures, such as the Security Information and Events Management (SIEM) systems. According to the National Institute of Standards and Technology (NIST), these systems are often ineffective for CIs protection. In this paper we analyze limits of current SIEMs and propose a framework developed in the MASSIF Project to enhance services for data treatment. Particularly, the Generic Event Translation (GET) module collects security data from heterogeneous sources, by providing intelligence at the edge of the SIEM; the Resilient Storage (RS), reliably stores data related to relevant security breaches. We illustrate a prototypal deployment for the dam monitoring and control case study.

Keywords: Security Information and Event Management (SIEM); Supervisory Control and Data Acquisition (SCADA); dam

[9] H. Debar, D. A. Curry, and B. S. Feinstein. The Intrusion Detection Message Exchange Format (IDMEF). RFC 4765 (Experimental), March 2007. [bib | http]

The purpose of the Intrusion Detection Message Exchange Format (IDMEF) is to define data formats and exchange procedures for sharing information of interest to intrusion detection and response systems and to the management systems that may need to interact with them.

This document describes a data model to represent information exported by intrusion detection systems and explains the rationale for using this model. An implementation of the data model in the Extensible Markup Language (XML) is presented, an XML Document Type Definition is developed, and examples are provided.

[10] M. El Maarabani. *Verification and test of interoperability security policies*. PhD thesis, Evry, Institut national des télécommunications, 2012. [bib]

Nowadays, there is an increasing need for interaction in business community. In such context, organizations collaborate with each other in order to achieve a common goal. In such environment, each organization has to design and implement an interoperability security policy. This policy has two objectives: (i) it specifies the information or the resources to be shared during the collaboration and (ii) it define the privileges of the organizations' users. To guarantee a certain level of security, it is mandatory to check whether the organizations' information systems behave as required by the interoperability security policy. In this thesis we propose a method to test the behavior of a system with respect to its interoperability security policies. Our methodology is based on two approaches: active testing approach and passive testing approach. We found that these two approaches are complementary when checking contextual interoperability security policies. Let us mention that a security policy is said to be contextual if the activation of each security rule is constrained with conditions. The active testing consists in generating a set of test cases from a formal model. Thus, we first propose a method to integrate the interoperability security policies in a formal model. This model specifies the functional behavior of an organization. The functional model is represented using the Extended Finite Automata formalism, whereas the interoperability security policies are specified using OrBAC model and its extension O2O. In addition, we propose a model checking based method to check whether the behavior of a model respects some interoperability security policies. To generate the test cases, we used a dedicated tool developed in our department. The tool allows generating abstract test cases expressed in the TTCN notation to facilitate its portability. In passive testing approach, we specify the interoperability policy, that the system under test has to respect, with Linear Temporal logics. We analyze then the collected traces of the system execution in order to deduce a verdict on their conformity with respect to the interoperability policy. Finally, we show the applicability of our methods though a hospital network case study. This application allows to demonstrate the effectiveness and reliability of the proposed approaches

[11] Guidelines for planning an integrated security operations center. Technical Report 3002000374, EPRI, Palo Alto, CA, Dec. 2013. http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000003002000374. [bib]

This report describes strategies and guidelines for utilities to plan and implement an Integrated Security Operations Center (ISOC) that includes corporate systems, control systems, and physical security. Currently, multiple groups and operators independently gather and analyze information from a datacenter, workstation networks, physical security, supervisory control and data acquisition (SCADA) systems, energy management systems (EMS), historians, and field equipment. Data is also collected and analyzed from Computer Emergency Readiness Teams (CERTs) and Information Sharing and Analysis Centers (ISACs). Correlating this data to find suspicious activity can be extremely challenging and often only occurs long after an incident happens.

An ISOC is designed to collect, integrate, and analyze alarms and logs from these traditionally siloed organizations, providing much greater situational awareness to the utilityâ€™s security team. Additionally, an ISOC allows utilities to transition to an intelligence-driven approach to incident management, which is much more effective for handling advanced threats. Because of these advantages, creating an ISOC may provide significant value to utilities. However, building an ISOC requires significant technical resources, staff, and time.

This research focuses on the initial steps in the process of setting up an ISOC: developing the business case, potential organizational challenges, tradeoffs for different ISOC architectures, and planning the implementation process. These results are based on current research, engagement with utilities, and an examination of ISOC implementations outside of the electric sector.

Keywords: Cyber Incident Management, Incident Detection System, Security Event Monitoring, Security Status Monitoring, Security and Information Event Management, Security Operations Center

[12] IntelliGrid Common Information Model Primer: Second Edition. Technical Report 3002001040, EPRI, Palo Alto, CA, Oct. 2013. http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000003002001040. [bib]

The Common Information Model (CIM) Primer explains the basics of the CIM (IEC 61970, IEC 61968, and IEC 62325). Starting with a historical perspective, it describes how the CIM originated and grew through the years. The functions of various working groups of Technical Committee 57 of the International Electrotechnical Commission (IEC) are described. The process of how an IEC standard is created is also outlined.

The basics of the Unified Modeling Language (UML) are detailed to introduce the reader to the language of the CIM. Then, building on commonly understood objects (basic shapes), the concepts that underline the CIM are carefully built step by step. The reader is then transported into the world of power systems where the concepts that were developed previously are applied to the complexities of the electric grid.

The Second Edition is updated with a case study that follows a utility through its journey of discovery, learning, and then, utilizing the CIM for grid modeling and integration. Additionally, questions have been added to the end of each section for the reader to reinforce their learning.

Keywords: Common Information Model (CIM), International Electrotechnical Commission (IEC), International standards Semantic model, Unified Modeling Language (UML)

[13] M. R. Grimaila, J. Myers, R. F. Mills, and G. Peterson. Design and analysis of a dynamically configured log-based distributed security event detection methodology. *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*, 9(3):219-241, 2012. [bib | DOI]

Military and defense organizations rely upon the security of data stored in, and communicated through, their cyber infrastructure to fulfill their mission objectives. It is essential to identify threats to the cyber infrastructure in a timely manner, so that mission risks can be recognized and mitigated. Centralized event logging and correlation is a proven method for identifying threats to cyber resources. However, centralized event logging is inflexible and does not scale well, because it consumes excessive network bandwidth and imposes significant storage and processing requirements on the central event log server. In this paper, we present a flexible, distributed event correlation system designed to overcome these limitations by distributing the event correlation workload across the network of event-producing systems. To demonstrate the utility of the methodology, we model and simulate centralized, decentralized, and hybrid log analysis environments over three accountability levels and compare their performance in terms of detection capability, network bandwidth utilization, database query efficiency, and configurability. The results show that when compared to centralized event correlation, dynamically configured distributed event correlation provides increased flexibility, a significant reduction in network traffic in low and medium accountability environments, and a decrease in database query execution time in the high-accountability case.

[14] P. Hui, J. Bruce, G. Fink, M. Gregory, D. Best, L. McGrath, and A. Endert. Towards efficient collaboration in cyber security. In *International Symposium on Collaborative Technologies and Systems*, pages 489-498, May 2010. [bib | DOI]

Cyber security analysts in different geographical and organizational domains are often largely tasked with similar duties, albeit with domain-specific variations. These analysts necessarily perform much of the same work independently- for instance, analyzing the same list of security bulletins released by largely the same set of software vendors. As such, communication and collaboration between such analysts would be mutually beneficial to the analysts involved, potentially reducing redundancy and offering the opportunity to preemptively alert each other to high-severity security alerts in a more timely fashion. However, several barriers to practical and efficient collaboration exist, and consequently, no such framework exists to support these efforts. In this paper, we discuss the inherent difficulties which make efficient collaboration between cyber security analysts a difficult goal to achieve. We discuss preliminary ideas and concepts towards a collaborative cyber-security framework currently under development, whose goal is to facilitate analyst collaboration across these boundaries. While still in its early stages, we describe work-in-progress towards achieving this goal, including motivation, functionality, concepts, and a high-level description of the proposed system architecture.

Keywords: groupware;security of data;collaboration;cyber security analysts;security bulletins;Collaboration;Collaborative software;Collaborative work;Computer security;Data security;Information analysis;Laboratories;Linux;Performance analysis;Software performance;Cyber-security systems;collaborative security frameworks;collaborative software frameworks;computer security

[15] K. Kent and M. P. Souppaya. Guide to computer security log management. Technical Report NIST Special Publication 800-92, Computer Security Division, Information Technology Laboratory, National Institute of Standards & Technology, Gaithersburg, MD, United States, Sept. 2006. [bib | http]

[16] S. Kowtha, L. Nolan, and R. Daley. Cyber security operations center characterization model and analysis. In *IEEE Conference on Technologies for Homeland Security (HST)*, pages 470-475, Nov. 2012. [bib | DOI]

While cyberspace knows no borders, there are commercial, regional, national and international interests that seek to assure the trust, availability and dependability of cyberspace for their specific needs. Cyber Security Operations is the term used to describe activities that span (a) securing a portion of cyberspace, (b) monitoring and analyzing threats and incidents, and (c) responsively and proactively managing incidents. These operations centers stand a better chance at securing and defending their portion of cyberspace if they adopt a collaborative and coordinated operations approach. In order to establish a strong analytical foundation required for developing collaborative cyber security operations tradecraft, an operations center characterization model is necessary to provide the common underlying framework for collaboration discussions. We have developed an analytical model to capture common and significant aspects of cyber security operations centers. The model addresses seven foundational areas or dimensions: scope, activities, process management, facilities, organizational dynamics, external interactions, and environment. We developed a simple, yet effective, operations center questionnaire based on the model, and used it to collect actual operations center data from a dozen diverse cyber security operations centers. In this paper we describe the operations center characterization model and discuss information gleaned from four of the cyber security centers. We demonstrate that the operations center characterization model's rapid data collection and visual analysis lends itself to aiding the cyber security community to (a) identify areas of collaboration, (b) customize information sharing, and (c) improve efficiency and effectiveness of a center's operations by learning from similar centers in the community

Keywords: groupware;security of data;system monitoring;trusted computing;collaboration discussion;collaborative cyber security operation;commercial interest;coordinated operation;cyber security operations center characterization model;cyberspace availability assurance;cyberspace dependability assurance;cyberspace trust assurance;data collection;effectiveness improvement;efficiency improvement;external interaction;incident analysis;information sharing;international interest;organizational dynamics;proactive incident management;regional interest;threat analysis;threat monitoring;visual analysis;Analytical models;Collaboration;Communities;Computer security;Cyberspace;Data models;Organizations;collaborative cyber security operations;coordinated incident response;cyber security activities;cyber security information sharing;operations center characterization model

[17] L. Kufel. Security event monitoring in a distributed systems environment. *IEEE Security & Privacy*, 11(1):36-43, Jan 2013. [bib | DOI]

Today, organizations depend much more on IT than they did in the past. Services such as internal portals, email communication, and financial and HR systems rely on computers to move businesses forward. These systems are under pressure to be securer than ever to protect organizations' operational environment. One aspect to consider in this situation is IT security event management. This article presents the design and implementation of two security event monitoring approaches in a distributed systems environment.

Keywords: distributed processing;security of data;HR systems;IT security event management;distributed systems environment;email communication;internal portals;operational environment;security event monitoring;Computer security;Distributed processing;Event detection;Information technology;Monitoring;Servers;Software engineering;distributed systems;events monitoring;monitoring on demand;security events

[18] S. T. Ludovice. Analysis of the impact of data normalization on cyber event correlation query performance. Master's thesis, Air Force Institute of Technology, Graduate School of Engineering and Management, Wright-Patterson Air Force Base, OH, Mar. 2012. [bib | http]

A critical capability required in the operation of cyberspace is the ability to maintain situational awareness of the status of the infrastructure elements that constitute cyberspace. Event logs from cyber devices can yield significant information, and when properly utilized they can provide timely situational awareness about the state of the cyber infrastructure. In addition, proper Information Assurance requires the validation and verification of the integrity of results generated by a commercial log analysis tool. Event log analysis can be performed using relational databases. To enhance database query performance, previous literatures affirm denormalization of databases. Yet database normalization can also increase query performance. Database normalization improved the majority of the queries performed using very large data sets of router events. In addition, queries performed faster on normalized tables when all the necessary data were contained in the normalized tables. Database normalization improves table organization and maintains better data consistency than a lack of normalization. Nonetheless, there are some tradeoffs when normalizing a database, such as additional preprocessing time and extra storage requirements. But overall, normalization improved query performance and must be considered an option when analyzing event logs using relational databases. There are three primary research questions addressed in this thesis: (1) What standards exist for the generation, transport, storage, and analysis of event log data for security analysis?; (2) How does database normalization impact query performance when using very large data sets (over 30 million) of router events?; and (3) What are the tradeoffs between using a normalized versus non-normalized database in terms of preprocessing time, query performance, storage requirements, and database consistency?

[19] J. Madrid, L. Munera, C. Montoya, J. Osorio, L. Cardenas, R. Bedoya, and C. Latorre. Functionality, reliability and adaptability improvements to the OSSIM information security console. In *IEEE Latin-American Conference on Communications (LATINCOM)*, pages 1-6, Sept. 2009. [bib | DOI]

Security consoles are among the most widely deployed tools for information security management in today's organizations. This article summarizes the work of our research team, in order to incorporate several enhancements to the OSSIM information security console. Such enhancements include integration with physical security control devices, automatic creation of correlation directives for OSSIM's correlation engine, and a significant improvement in information capture reliability on high-traffic networks.

Keywords: security of data;OSSIM;high-traffic networks;information capture reliability;information security console;information security management;physical security control devices;Automatic control;Computer architecture;Detectors;Engines;Force measurement;Information management;Information security;Intrusion detection;Pattern analysis;Software tools;Information security;OSSIM;alert correlation;physical security;security consoles

[20] A. Mercer. Security information and event management for small and medium-sized enterprises. Master's thesis, Luleå University of Technology, Department of Computer science, Electrical and Space engineering, 2013. [bib]

Purpose-This research project sets out to identify the security event management problems perceived in the SME context, prioritise these problems and then seek to solve them through the design and implementation of a prototype Security Information and Event Management (SIEM) system.

Design/Methodology/Approach-Action Design Research (ADR) is the research methodology used in this research project. ADR combines Action Research (AR) and Design Science (DS) research to solve a problem situation in a specific organisational setting through intervention and evaluation as well as the construction and evaluation of a novel IT artefact. A prototype SIEM was successfully

designed and implemented in the case organisation over the course of a ten week intervention.

Findings-A number of findings emerged related to the testing of Design Principles (DPs) extracted from earlier SIEM research, the testing of ADR in the context of an SME as well as the presentation of nine new DPs for SIEM design and implementation in similar future projects.

Practical Implications-Apart from a working prototype SIEM in the SME context one output from the research project is a planning and implementation checklist for practitioners for future SIEM design and implementation projects, generalizable to all contexts and not just that of the SME.

Originality/Value-This research provides a short state-of-the-art summary of current SIEM research, validates two DPs extracted from earlier SIEM research, proposes nine new DPs relevant to future SIEM design and implementation and tests the effectiveness of ADR in the context of an SME research project.

Keywords: Security Information Event Management (SIEM), Small and Medium Enterprise (SME), Action Design Research (ADR), Design Principles (DP)

[21] R. Montesino, S. Fenz, and W. Baluja. SIEM-based framework for security controls automation. *Information Management & Computer Security*, 20(4):248-263, 2012. [bib | DOI]

Purpose-The purpose of this paper is to propose a framework for security controls automation, in order to achieve greater efficiency and reduce the complexity of information security management.

Design/methodology/approach-This research reviewed the controls recommended by well known standards such as ISO/IEC 27001 and NIST SP 800-53; and identified security controls that can be automated by existing hard-and software tools. The research also analyzed the Security Information and Event Management (SIEM) technology and proposed a SIEM-based framework for security controls automation, taking into account the automation potential of SIEM systems and their integration possibilities with several security tools.

Findings-About 30 percent of information security controls can be automated and they were grouped in a list of ten automatable security controls. A SIEM-based framework can be used for centralized and integrated management of the ten automatable security controls.

Practical implications-By implementing the proposed framework and therefore automating as many security controls as possible, organizations will achieve more efficiency in information security management, reducing also the complexity of this process. This research may also be useful for SIEM vendors, in order to include more functionality to their products and provide a maximum of security controls automation within SIEM platforms.

Originality/value-This paper delimits the boundaries of information security automation and defines what automation means for each security control. A novel framework for security controls automation is proposed. This research provides an automation concept that goes beyond what it is normally described in previous works and SIEM solutions.

Keywords: Computer security, Data security, Information management, Information security management, Security automation, Security information and event management

[22] A. V. Pantola, J. P. Encarnacion, J. D. G. Pineda, and R. F. Y. Jr. Normalization of logs for networked devices in a security information event management system. justinspeaks.files.wordpress.com/2010/10/device-normalizer-paper.pdf, 2010. [bib]

[23] S. Reißmann, D. Frisch, and S. Rieger. Automatisierte Korrelation und Aggregation von Syslog-Nachrichten in NoSQL-basierten Datenbanken. In P. Müller, B. Neumair, H. Reiser, and G. D. Rodosek, editors, *6. DFN-Forum Kommunikationstechnologien, Beiträge der Fachtagung*, volume 217 of *Lecture Notes in Informatics (LNI)*, pages 21-30. German Informatics Society (GI), June 2013. [bib | .pdf]

[24] R. Rieke, L. Coppolino, A. Hutchison, E. Prieto, and C. Gaber. Security and reliability requirements for advanced security event management. In I. Kotenko and V. Skormin, editors, *Computer Network Security*, volume 7531 of *Lecture Notes in Computer Science*, pages 171-

180. Springer Berlin Heidelberg, 2012. [bib | DOI]

> With the growing size and complexity of current ICT infrastructures, it becomes increasingly challenging to gain an overview of potential security breaches. Security Information and Event Management systems which aim at collecting, aggregating and processing security-relevant information are therefore on the rise. However, the event model of current systems mostly describes network events and their correlation, but is not linked to a comprehensive security model, including system state, security and compliance requirements, countermeasures, and affected assets. In this paper we introduce a comprehensive semantic model for security event management. Besides the description of security incidents, the model further allows to add conditions over the system state, define countermeasures, and link to external security models.
>
> Keywords: security requirements; security information and event management; SIEM; architecting trustworthy systems

[25] J. Schütte, R. Rieke, and T. Winkelvos. Model-based security event management. In I. Kotenko and V. Skormin, editors, *Computer Network Security*, volume 7531 of *Lecture Notes in Computer Science*, pages 181-190. Springer Berlin Heidelberg, 2012. [bib | DOI]

> With the growing size and complexity of current ICT infrastructures, it becomes increasingly challenging to gain an overview of potential security breaches. Security Information and Event Management systems which aim at collecting, aggregating and processing security-relevant information are therefore on the rise. However, the event model of current systems mostly describes network events and their correlation, but is not linked to a comprehensive security model, including system state, security and compliance requirements, countermeasures, and affected assets. In this paper we introduce a comprehensive semantic model for security event management. Besides the description of security incidents, the model further allows to add conditions over the system state, define countermeasures, and link to external security models.
>
> Keywords: security strategy meta model; security information and event management; complex event processing

[26] Understanding and Selecting SIEM/LM: Aggregation, Normalization, and Enrichment. https://securosis.com/blog/understanding-and-selecting-siem-lm-aggregation-normalization-and-enrichmen, retrieved Mar 4, 2014. [bib]

[27] T. Sommestad, G. Ericsson, and J. Nordlander. SCADA system cyber security - A comparison of standards. In *IEEE Power and Energy Society General Meeting*, pages 1-8, July 2010. [bib | DOI]

> Cyber security of Supervisory Control And Data Acquisition (SCADA) systems has become very important. SCADA systems are vital for operation and control of critical infrastructures, such as the electrical power system. Therefore, a number of standards and guidelines have been developed to support electric power utilities in their Cyber security efforts. This paper compares different SCADA Cyber security standards and guidelines with respect to threats and countermeasures they describe. Also, a comparison with the international standard ISO/IEC 17799 (now ISO/IEC 27002) is made. The method used is based on a comparison of use of certain key issues in the standards, after being grouped into different categories. The occurrences of the key issues are counted and comparisons are made. It is concluded that SCADA specific standards are more focused on technical countermeasures, such as firewalls and intrusion detection, whereas ISO/IEC 17799 is more focused on organizational countermeasures.
>
> Keywords: IEC standards;ISO standards;SCADA systems;security of data;Cyber security;ISO/IEC 17799;SCADA system;electrical power system;international standard;supervisory control and data acquisition system;technical countermeasure;Control systems;Cyber Security;SCADA systems;Smart Grids;Standards

[28] K. Stouffer, J. Falco, and K. Scarfone. Guide to industrial control systems (ICS) security. *NIST Special Publication*, 800:82, Sept. 2007. [bib]

[29] K. Stroeh, E. Mauro Madeira, and S. Goldenstein. An approach to the correlation of security

events based on machine learning techniques. *Journal of Internet Services and Applications*, 4(1):1-16, 2013. [bib | DOI]

Organizations face the ever growing challenge of providing security within their IT infrastructures. Static approaches to security, such as perimetral defense, have proven less than effective â€” and, therefore, more vulnerable â€” in a new scenario characterized by increasingly complex systems and by the evolution and automation of cyber attacks. Moreover, dynamic detection of attacks through IDSs (Instrusion Detection Systems) presents too many false positives to be effective. This work presents an approach on how to collect and normalize, as well as how to fuse and classify, security alerts. This approach involves collecting alerts from different sources and normalizes them according to standardized structures â€” IDMEF (Intrusion Detection Message Exchange Format). The normalized alerts are grouped into meta-alerts (fusion, or clustering), which are later classified using machine learning techniques into attacks or false alarms. We validate and report an implementation of this approach against the DARPA Challenge and the Scan of the Month, using three different classifications â€” SVMs, Bayesian Networks and Decision Trees â€” having achieved high levels of attack detection with little false positives. Our results also indicate that our approach outperforms other works when it comes to detecting new kinds of attacks, making it more suitable to a world of evolving attacks.

Keywords: IDS; Security; Correlation; Machine learning

[30] H. Suleiman and D. Svetinovic. Evaluating the effectiveness of the security quality requirements engineering (SQUARE) method: a case study using smart grid advanced metering infrastructure. *Requirements Engineering*, 18(3):251-279, 2013. [bib | DOI]

This paper presents an evaluation of the security quality requirements engineering (SQUARE) method. The evaluation of SQUARE was conducted by its application on the advanced metering infrastructure of smart grid as a case study. We evaluated the effectiveness of SQUARE with respect to its ability to elicit a set of artifacts, threats, and vulnerabilities; to perform likelihood, impact analysis, and risk level determination; and to elicit, categorize, and prioritize the security requirements. The main contribution of this work is the evaluation of the effectiveness of SQUARE using qualitative security requirements engineering method evaluation criteria.

Keywords: Security requirements engineering method evaluation; Advanced metering infrastructure (AMI) security; Smart grid security; Security quality requirements engineering (SQUARE) method; Qualitative research evaluation

[31] D. Wei, Y. Lu, M. Jafari, P. Skare, and K. Rohde. Protecting smart grid automation systems against cyberattacks. *IEEE Transactions on Smart Grid*, 2(4):782-795, Dec. 2011. [bib | DOI]

The smart grid moves new power grid automation systems from being proprietary and closed to the current state of information technology (IT) which is highly interconnected and open. But open and interconnected automation platforms bring about major security challenges. The power grid automation network has inherent security risks due to the fact that the systems and applications for the power grid were originally designed without much consideration of cybersecurity. This paper first introduces scope and functionalities of power grid, its automation and control system, and communications. Potential cyberattacks and their adverse impacts on power grid operation are discussed, a general SCADA cyberattack process is presented. This paper discusses the major challenges and strategies to protect smart grid against cyberattacks and finally proposes a conceptual layered framework for protecting power grid automation systems against cyberattacks without compromising timely availability of control and signal data. The proposed “bump-in-the-wire” approach also provides security protection for legacy systems which do not have enough computational power or memory space to perform security functionalities. The on-site system test of the developed prototype security system is briefly presented as well.

Keywords: SCADA systems;information technology;power system protection;power system security;risk analysis;smart power grids;IT;SCADA cyberattack process;bump-in-the-wire approach;conceptual layered framework;cybersecurity;information technology;interconnected automation platforms;on-site system test;power grid automation network;power grid automation systems;prototype security system;security risks;signal data;smart grid automation system protectionz;Computer crime;Computer security;Network security;Quality of service;Substations;Quality-of-Service (QoS);Smart grid;cyberattacks;network security;vulnerability

This file was generated by bibtex2html 1.96.