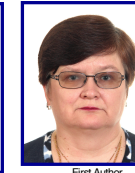


#31



Network Security Intelligence Centres for Information Security Incident Management

Miloslavskaya N. (namiloslavskaya@mephi.ru) NRNU MEPhI, Moscow, Russia, **Furnell S.** Plymouth University, UK



ABSTRACT

Intensive IT development is driving current information security (IS) trends and require sophisticated structures and adequate approach to manage IS for different businesses. The wide range of threats is constantly growing in modern intranets; they have become not only numerous and diverse but also more disruptive. In such circumstances, organizations realize that IS incidents' timely detection and prevention in the future (what is more important) are not only possible but imperative. Any delay leaves only reactive actions to IS incidents, putting assets at risk as a result. A properly designed IS incident management system (ISIMS), operating as an integral part of the whole organization's governance system, reduces IS incidents' number and limits damage caused by them. To maximally automate IS incident management (ISIM) within one organization and to deepen its knowledge of IS level, this research proposes to unite together all advantages of a Security Intelligence Centre (SIC) and a Network Operations Centre (NOC) with their unique and joint toolkits and techniques in a unified Network SIC (NSIC). This paper presents the research, which is focused upon the designing and evaluating the concept of NSICs, and represents a novel advancement beyond existing concepts of security and network operations centres in current security monitoring scenarios. Key contributions are made in relation to underlying taxonomies of threats and attacks, leading to the requirements for NSICs, the related design, and then evaluation in a practical context and the implications arising from this (e.g. training requirements).

INTRODUCTION

Intensive IT development is driving current information security (IS) trends and requires sophisticated structures and adequate approach to manage IS for different businesses. The range of threats has become more numerous and diverse as well as more disruptive. In such circumstances, modern organisations get a huge amount of data about the current state of their IT infrastructures (ITIs) and at a first glance much of this may seem unrelated (with scattered events taking place). This data needs to be processed correctly and promptly to identify IS incidents and to highlight ITI areas being at high risk. The ever-increasing volumes and heterogeneity of data and related activity for scrupulous analysis are very high. No matter how dedicated and talented, security staff cannot keep up with the volume of data flowing through the organisation's ITI and the speed with which things related to IS happen. A problem of structured, consolidated, and visual presentation of data to make timely and informed decisions in ensuring ITI's IS rises very sharply. A unified, inclusive, scalable, and effective system with required 'best-of-breed' IPTs will allow security analysts to truly manage IS for their ITIs. Such a system with proper Security Intelligence (SI) services in place will help to mitigate and promptly respond to IS threats by helping organisations better understand their landscape and to perform routine work without the involvement of professionals in automatic mode. It will do this through the gathering, analysis, and filtering of raw IS-related data that are then will be collected into appropriate databases, will be presented in management reports with necessary visualisation and will be transferred for IPTs reconfiguring and online IS monitoring.

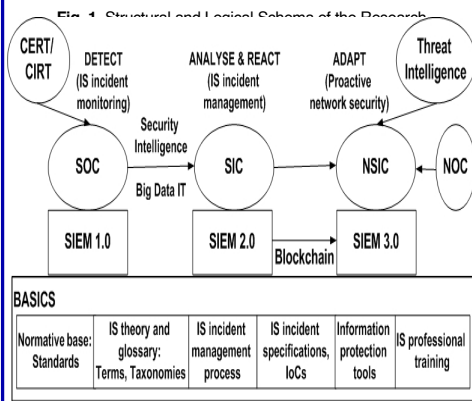
To automate IS incident management (ISIM) within one organisation it is proposed to unite together all advantages of a Security Intelligence Centre (SIC) and a Network Operations Centre (NOC) with their unique and joint toolkits and techniques in a Network SIC (NSIC).

Research Aims

Based upon the above, the goal of the research is to develop and start to implement the concept for a new state-of-the-art centralised network security management unit called NSIC intended to increase the effectiveness of ISIM processes (ISIMP) for modern organisations to be proactive and resilient to damaging IS threats as their urgent and priority need. In its simplest way, the drive to carry out this research can be reduced to two research questions as follows: How this NSIC should be designed? What knowledge and skills should an IS professional working there have?

The creation of the innovative NSIC concept, its interpretation and construction through original research will contribute substantially to the modern networks' security, as it will extend the forefront of the main security measures and tools used nowadays.

The research methodology is firmly based on the scientific management theory, general system theory, open information system and big data IT concepts, as well as proposed IS theory basics. The applicable techniques for the research are the well-known analytical approaches, namely system analysis of the object of research, which allows to carry out its complex modelling; exploratory research, analysis, systematisation and classification of typical network vulnerabilities, IS threats, attacks and IS incidents; process approach used to describe the monitoring of IS for modern networks; comparative analysis of two generations of Security Information and Event Management (SIEM) systems as well as Security Operations Centres (SOCs) and SICs, synthesis of requirements for a NSIC for centralised IS monitoring in modern networks, taking into account the main provisions of management theory and identifying its closest counterparts; synthesis of requirements for a next-generation SIEM 3.0 system as a core of the NSIC, development of a glossary of key terms used, etc. As for any research, some grounded assumptions were made. The research made a few assumptions as follows: ITIs are considered only from the wired network viewpoint since the research was started at the time when wireless technologies were not being used as widely as at present; The research focus was on the technical aspects of NSIC's design (not its documentation support) because it is more relevant to the competences and qualification of the author of this research; A private (not cloud-based, without outsourcing) NSIC is proposed because it presupposes a cruder elaboration of all the issues of NSIC support by its owner.



IS theory development

Using the glossary proposed and analysing real-world attacks (like APTs, phishing e-mails, pharming, scams, DoS attacks, XSS, SQL injections, targeted watering hole attacks, ransomware, Heartbleed, ShellShock) and numerous reports of well-known companies (like PricewaterhouseCoopers, Symantec, Endescan, CA technologies, Flexera), our own taxonomy with classifications of network vulnerabilities, IS threats, attacks, and incidents is proposed. The main classification parameters defined are the following:

For a vulnerability: its origin sources, allocation in ITI, risk level (criticality, severity), probability/likelihood of a threat realisation on its basis and prerequisites;

For an IS threat: its type (according to a violation of physical integrity, logical structure, content, confidentiality, property rights, availability, privacy, etc.), origin nature, prerequisites, and sources;

For an attack: influence type (passive or active), aim, condition of influence beginning (on request, on event occurrence or unconditional), allocation of a victim and an attacker (in one or different network segments), number of victims and attackers (traditional or distributed), feedback presence (with or without feedback), implementation level according to the seven-layer ISO/OSI model, implementation tools (information interchange, commands, scripts, etc.), implementation form (sniffing, masquerade, spoofing, hijacking, phishing, pharming, etc.) and so on; For an IS incident: type, priority, malefactor (malefactors), aims to be achieved, methods and tools that can be used, actions and targeted objects on which these actions are directed, affected objects and particular information assets, impact and its severity, detection and response complexity, etc.

To continue, the most important 28 verbal descriptions of the signs of remote attacks, better known as Indicators of Compromise (IoCs), were worked out. They are related to the typical activities/their combination associated with a specific attack, for example: unauthorised user on the network/shared credentials; unauthorised access to confidential data, Personally Identifiable Information (PII) and financial data; unauthorised internal host connection to the Internet; excessive access from single/multiple internal hosts to external malicious website (from the blacklists); off-hour (at night/on weekends) user's activity and malware detection; multiple logins with the same ID from different locations in a short time; internal hosts communicate either with known untrusted destinations or to the hosts allocated in another country where there are no organisation's business partners or to external hosts using non-standard ports or protocol/port mismatches; a single host/user account tries to log in to multiple hosts within network a few minutes from/to different regions; etc.

From our taxonomy, it is obvious that IS incidents can be described in completely different ways. That is why there are many standards, which are designed for unifying these descriptions. Among the most known are the following data exchange specifications: IODEF and RID by the MILE working group; IDMEF and IODEF-SCI by IETF; CIF by REN-ISAC; VERIS by Verizon; OpenIOC by Mandiant; OTX by Alien Vault; CyBox, TAXII and STIX by MITRE. The last three standards were selected to form a unified template for IS incident description for SIEM 3.0.

CONCLUSIONS

The aim of the research was to develop and start to implement the concept of a new state-of-the-art centralised network security management unit called NSIC. To achieve the goal, all the solutions proposed were considered from different angles and at the same time as a whole. To that end, one can be confident that the NSIC developed at an advanced level suitably meets its purpose. This is due to the fact that the proposed concept and its description give the high-level guidelines that will help organisations (from small to large) to plan, implement and evaluate their in-house NSICs.

Future plans for the framework include the development and subsequent implementation of educational standards, and competency models for different educational levels for specialised network security professional training. The centre is also expected to carry out research on the NSIC's design, effective network security management practices based on SI approaches and applications, the study of the compatibility between different IPTs, and recommendations to address arising issues in terms of evaluating network security.

NSICs

At present, even this perspective idea of SICs does not keep pace with the increasing number of sophisticated IS threats in the highly heterogeneous and connected world. A new entity to be designed should unite all benefits of SIC with many-year experience of network operations management, namely change the security model from reactive to proactive, support more informed and effective responses to IS incidents, enhance communications between the network and security teams, management and board members, and drive IS investment strategies and connect more directly IS priorities with business risk management priorities. Therefore, a new NSIC's concept as a SIC-NOC combination is proposed in the research.

The NSIC introduces powerful synergies of SICs and NOCs via people collaboration and toolkits and techniques joint usage. Some of the significant benefits of NSICs to their owners are the following:

- Complete situational awareness with seamless integration of the monitored entities from network and SI services with a supporting infrastructure;
 - Network and security real-time monitoring, meeting IS management requirements;
 - Centralised network devices' and IPTs' configuration management and audit;
 - Computer-based data collection and analytics from both network and IS viewpoints to extract maximum value from the massive amounts of IS-related data;
 - IPTs alerts' prioritisation; richer organisation-wide context mining to aid operational and strategic IS decision-making and to validate that the right IS policies are in place;
 - Faster IS event detection and reduced IS incident response times by automated remediation and enabling IS controls and IT to work together;
 - Advanced network forensics;
 - Actionable streamlined ISIM (including behavioural analytics for continuous monitoring, pre/post analysis) and reporting with valuable context.
- The main specific requirements, which should be taken into account in designing NSICs, was formulated as follows:
- NSIC processes should be in line to industry regulations and applicable standards;
 - Usage of more types of data for analytics;
 - Modular and adaptive IS event management achieved;
 - Operational resilience, scalability, elasticity, maintainability, agility, IS, trustworthy.
 - Compliance with these requirements of the NSIC proposed was proven.
- The well-known Deming-Shewhart Wheel or PDCA/PDSA cycle was chosen as the NSIC's development methodology. The most important issues for the training of highly qualified staff for NSICs were also discussed.

Considering a separate IS event, it is proposed to visualise for decision-making in NSICs the following information: Who: access subject; Why: involuntary or unintentional action (error), ignorance, negligence or irresponsibility, malicious actions, etc.; What: unauthorised access to a system and/or information, installing unauthorised programs without consent of the owner, remote causing malfunction in the information system, stressful situation creation, physical intrusion, illegal activities, breakdown or failure of equipment, etc.; How: methods and tools for each of the above "what"; status of the IS event: an attempt, a successful or failed hacking; Which vulnerability was exploited: software, hardware, general protection, system architecture or processes, etc.; On which type of assets (basic and related); what are the consequences: violation of confidentiality, integrity, availability, etc.

A layered infrastructure with 5 layers (platform, software, service delivery, access, and management) and zone security infrastructure with 4 zones (demilitarized, trusted, restricted and management) was proposed.

A blockchain-based SIEM 3.0 system for the NSIC as its core and the resulting system's architecture, completely assigned with the SI concept, were proposed. We have a short-term experience in implementing NSIC's concept in the "Network Security Intelligence Centre" educational and research centre established in 2016 within the framework of the MEPhI's Institute of Cyber Intelligence Systems. Its goal is to implement a model of NSIC for its study and continuous improvement. The MEPhI's NSIC is based on three bearing laboratories with NGWFS, Data Loss Prevention (DLP) and SIEM systems at their cores respectively used at present for educational purposes (because the hardware and software base of the centre is still not fully developed for research purposes).