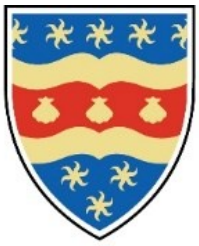
2019

Network Security Intelligence Centres for Information Security Incident Management

Miloslavskaya, Natalia



UNIVERSITY OF
PLYMOUTH

NETWORK SECURITY INTELLIGENCE CENTRES

FOR INFORMATION SECURITY INCIDENT MANAGEMENT

by

NATALIA MILOSLAVSKAYA

A thesis submitted to the University of Plymouth
in partial fulfilment for the degree of

DOCTOR OF PHILOSOPHY

School of Computing, Electronics and Mathematics

May 2019

Table of Contents

List of Figures

List of Tables

Author's Declaration

At no time during the registration for the degree of Doctor of Philosophy has the author been registered for any other University award without prior agreement of the Doctoral College Quality Sub-Committee.

Work submitted for this research degree at the University of Plymouth has not formed part of any other degree either at the University of Plymouth or at another establishment.

Word count of the main body of thesis: 15984.

Signed 

Date December 19, 2018

Acknowledgements

The works that form the basis for this research were created while under the employment of the National Research Nuclear University MEPhI (Moscow Engineering Physics Institute) while working as Associate Professor based in Moscow, Russia. The papers were published in the form of journal and conference papers that have been peer reviewed by relevant experts in the field to ensure novelty, efficacy and value.

Glossary of Abbreviations

APT	Advanced Persistent Threat
ARP	Address resolution protocol
CSRF	Cross Site Request Forgery
DB	Database
DBMS	Database management system
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DLP	Data loss prevention
DMZ	Demilitarised zone
DNS	Domain Name System
DoS	Denial of Service
ICT	Information and communication technologies
IoC	Indicator of Compromise
IP	Internet Protocol
IPT	Information protection tool
IS	Information security
ISIM	Information security incident management
ISIMP	Information security incident management process
ISIMS	Information security incident management system
ISIRT	Information security incident response team
IT	Information technologies
ITI	Information technologies infrastructure
KPI	Key Performance Indicators
MAC	Media Access Control
MiTM	Man-in-the-Middle
NGFW	Next Generation Firewall
NOC	Network Operations Centre
NSIC	Network Security Intelligence Centre
OS	Operating system
SI	Security Intelligence

SIC	Security Intelligence Centre
SLA	Service Level Agreement
URL	Uniform Resource Locator
XSS	Cross Site Scripting

Abstract

Network Security Intelligence Centres for Information Security Incident Management

Natalia Miloslavskaya

Intensive IT development has led to qualitative changes in our living, which are driving current information security (IS) trends and require sophisticated structures and adequate approached 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 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 and only reactive actions to IS incidents put their assets under risk.

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). For this purpose the glossary of the research area was introduced, the taxonomy of IS threats, vulnerabilities, network attacks, and incidents was determined. Further, IS monitoring as one of the ISIM processes was described, the Security Information and Event Management (SIEM) systems' role in it and their evolution were shown. The transition from Security Operations Centres (SOCs) to SICs was followed up. At least, modern network environment's requirements for new protection solutions were formulated and it was proven that the NSIC proposed as a combination of a SIC and a NOC fully meets them. The NSIC's zone security infrastructure with corresponding IS controls is proposed. Its implementation description at the Moscow Engineering Physics Institute concludes the research at this stage. In addition, some proposals for the training of highly qualified personnel for NSICs were formulated.

The creation of an innovative NSIC concept, its interpretation, construction and initial implementation through original research presented are its main results. They contribute substantially to the modern networks' security, as they extend the forefront of the SOCs and SICc used nowadays and generate significant new knowledge and understanding of network security requirements and solutions.

1 Introduction

1.1 Background

Intensive development of information technologies (IT) has led to qualitative changes in economic, socio-political and spiritual spheres of public life. These dramatic changes are driving current information security (IS) trends and require sophisticated structures and adequate approached to manage IS for individuals, organisations, and countries. The wide range of IS threats, especially those related to new network technologies, is constantly growing (Fig. 1) [Hackmaggedon, 2018]; they have become not only numerous and diverse but more disruptive.

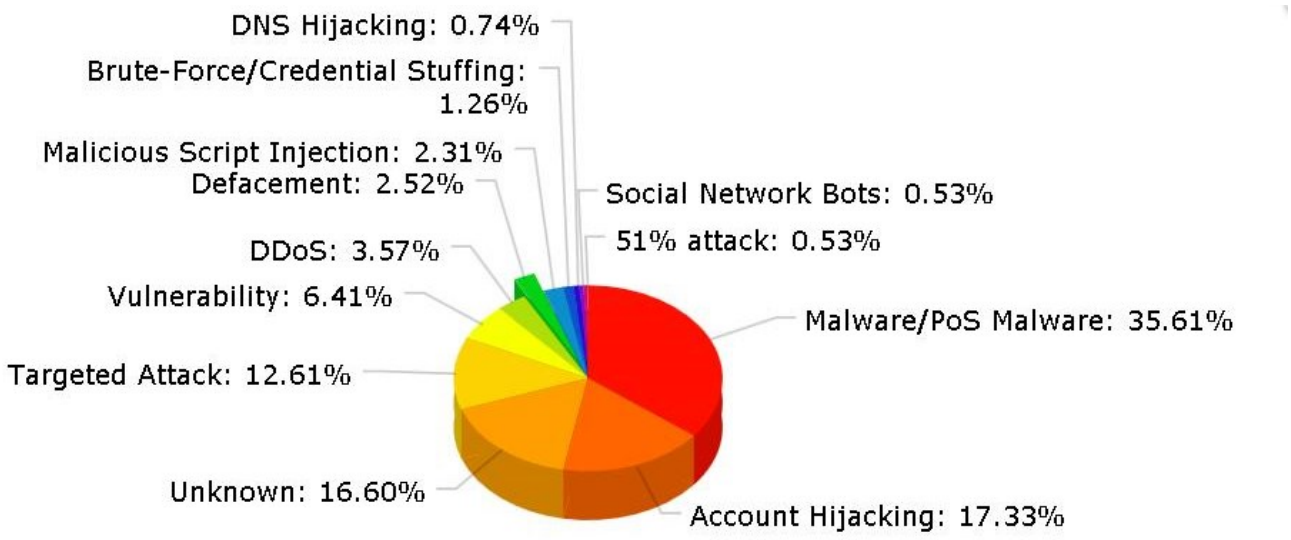


Figure 1. January-October 2018 Top 10 attacks [from hackmageddon.com]

In these circumstances, organisations begin to realise that IS incidents' timely detection and what is more important prevention in the future is not only possible but imperative. Any delay and only reactive actions to IS incidents put organisations' assets under risk. Properly designed and operating IS incident management (ISIM) system as an integral part of the whole organisation's governance system reduces IS incidents' number and limits damage caused by them.

Modern organisations get a huge amount of data about the current state of their IT infrastructures (ITIs) and unrelated (scattered) at a first glance events taking place in them. These data need to be processed correctly and promptly to identify IS incidents and to highlight ITI areas being at high risk for its rapid elimination. The data are coming not just from the separate domain controllers, proxy servers, Domain Name System (DNS) servers, information protection tools (IPTs), but also describe current configurations of network devices, characteristics of network traffic, application and network services functioning, activity and specific actions of individual end-users, as well as contain e-mails, phone records, web-based content, metadata, digitised audio and video, GPS locations, data of business processes, organisation's internal documents and analytical data for many years of its existence [P03]. All these IS-related data should be considered in a particular context and evaluated online from a viewpoint of any IS incident to find its source, consider its type, weight its consequences, visualise its vector, associate all target systems, prioritise countermeasures and offer mitigation solutions with weighted impact relevance. It is vital to know what IS threats exist at the moment, how they could grow into IS incidents and then affect organisations, especially if they could result in the exposure of intellectual property and confidential data or service interruption, jeopardise reputation or financial well-being, etc.

The ever-increasing volumes and heterogeneity of data and related activity for further scrupulous monitoring and 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 all the necessary "best-of-breed" tools and measures will allow security analysts to truly manage IS for their organisations' ITIs [P03]. Such a system with proper security intelligence 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 that does not require 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 different types of visualisation and will be transferred for IPTs reconfiguring and online IS monitoring and control.

To automate ISIM maximally within one organisation and to deepen its knowledge of ITI 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 unified Network SIC (NSIC) [P09], [P15].

1.2 Research Aims

Based upon the above, *the goal of the research* is to develop and begin to implement a concept of a new state-of-the-art centralised network security management unit called NSIC intended to increase the effectiveness of ISIM processes 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? And 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 [Taylor, 1998], general system theory [Bertalanffy, 1968], open information system concept [ISO/IEC, 10165-1], big data IT concept [Lynch, 2008] and proposed IS theory basics [P04]. 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 new unit (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.

It is natural that any research cannot go without making some *grounded assumptions*. The research made a few assumptions as follows:

1) ITIs are considered only from the wired network viewpoint since the research was conducted at the time when wireless technologies had just emerged, and were not being used as widely as at present;
2) The main attention of the research is made to 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;
3) A private (not cloud-based and without outsourcing) NSIC is proposed because it presupposes a cruder elaboration of all the issues of NSIC support by the centre's organization-owner.

1.3 Thesis structure

The following structure of the thesis is proposed in order to link closer prior published works in one holistic research to achieve the above goal.

Section 2 introduces some necessary terms and concepts as well as a special wording for describing unsecure ITI's state in terms of possible IS incidents, which should be detected and avoided in the future. Based on the results of Section 3, ISIM process (ISIMP) with special attention to IS monitoring in it is described, showing what IS-related data should be managed in ISIM and approving that it can be characterised as a big data. Discussion on SIEM systems as a core tool for ISIM concludes Section 3. Section 4 is devoted to SOCs' mission in IS monitoring as well as to their types and limitations. The Security Intelligence (SI) approach is discussed in Section 5, used further for NSIC's design as one of the basic concepts. Section 6 presents the main results of the research: in particular, the new NSIC's concept as a combination of a SIC and a NOC, the methodology of NSIC's development, its implementation in the specialised NSIC of the National Research Nuclear University MEPhI (Moscow Engineering Physics Institute) with a layered infrastructure and a zone security infrastructure and some issues, the solution of which supports its operations (for example, network security information to be visualised in NSICs, blockchain-based SIEM system for NSICs (called SIEM 3.0) and training of highly qualified staff for NSICs). Section 7 summarizes the

thesis by reiterating the contributions made by this research and the concluding remarks with suggestions for future research.

The corresponding structural and logical schema of the research conducted can be illustrated by Fig. 2, where CERTs/CIRTs (Computer Emergency Response Teams/Computer Incident Response Teams) were the structures that were in some sense forerunners for SOCs regarding its staff. It also emphasizes the main mottos of SOCs (DETECT IS incidents via constant monitoring), SICs (ANALYSE & REACT for real-time IS incident management) and proposed NSICs (ADAPT for proactive network security).

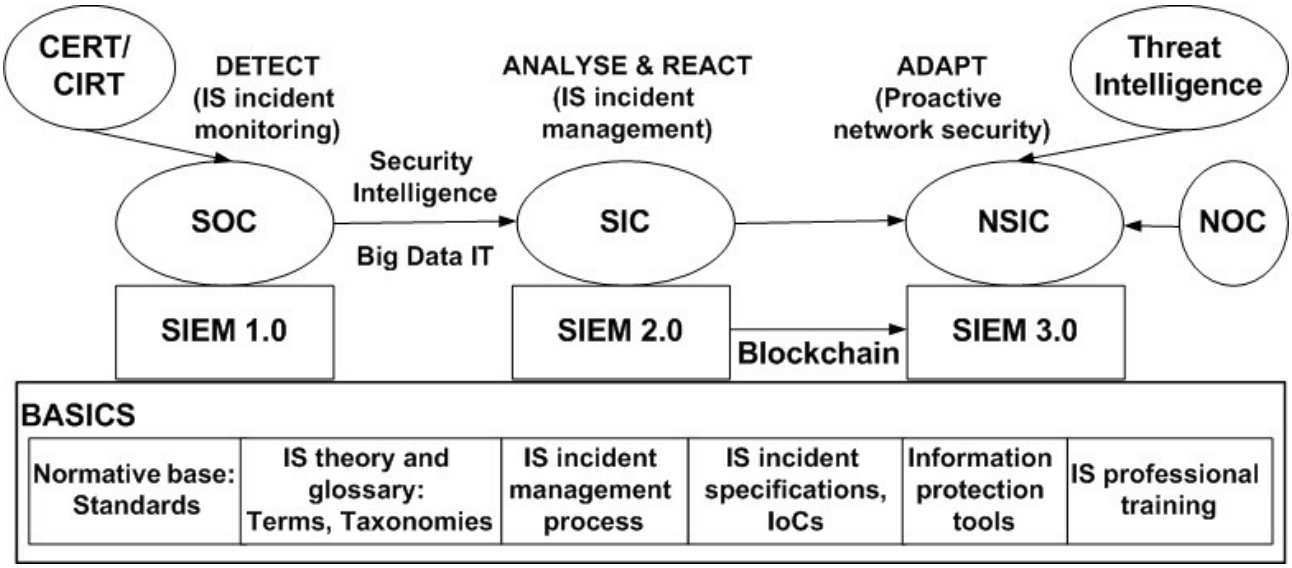


Figure 2. Structural and Logical Schema of the Research

The main body of the thesis is followed by an Appendix containing the Abstracts of each of the contributing publications (they are also listed in the first part of the References Section with the title and full bibliographic details of each). This also indicates the research contribution of each publication, and confirms the author's individual share of the contribution in each case.

The thesis's structure with an indication of the works, on which each section's content is based, is presented in Table 1. Further, the contribution of each section to the research and the lists of results obtained will be presented briefly with the indication of a prior published work.

Table 1. Thesis structure and contributing published works

Thesis section	Contributing Publications
Section 1. IS theory development	
1. IS terminology and IS concept	[P01], [P04]
2. IS threats, vulnerabilities, attacks and incidents taxonomy	[P07], [P12]
3. Key indicators of network attacks and their implementation as IS incidents	[P05], [P12]
4. Specifications unifying the information formats applicable to IS incident description	[P14]
Section 2. IS incident management (ISIM)	
1. ISIM process and subprocesses	[P01]
2. Role of IS monitoring in ISIM	[P02]
3. IS-related data to be managed in ISIM	[P03], [P13]
4. Application of big data, fast data and data lakes to IS-related data	[P06]
5. Security Information and Event Management (SIEM) system as a core tool for ISIM	[P10], [P14]
Section 3. Mission of Security Operations Centres (SOCs) in IS monitoring	
1. SOC with SIEM 1.0 system for IS incident monitoring	[P05], [P08], [P10], [P13]
2. SOC types	[P05]
3. SOC limitations	[P08], [P13]
Section 4. Mission of Security Intelligence Centres (SICs) in IS management	
1. SI concept and SIC with SIEM 2.0 system for IS management	[P08], [P11], [P13]
2. SIC's business logics	[P11]
3. SIC's data architecture and big data processing in SICs	[P11]
Section 5. Network Security Intelligence Centres (NSICs)	
1. Requirements for NSICs	[P15]
2. NSIC as a combination of a SIC and a NOC	[P15]
3. Network security information to be visualised in NSICs	[P02]
4. The methodology of NSIC development	[P16]
5. NSIC's layered infrastructure	[P16]
6. NSIC's zone security infrastructure	[P16]
7. NSIC's implementation in the MEPhI	[P09], [P18]
8. Blockchain-based SIEM 3.0 system for NSICs	[P14]
9. Training of highly qualified staff for NSICs	[P09], [P17], [P18], [P19], [P20]

2 IS theory development

At a time when the media constantly reports on new sophisticated attacks, organisations of any business and size need to prepare for such attacks against their ITIs. To counteract them organisations should have a properly designed IS management system with appropriate documentary support. IS policies for different application areas, including ISIM policy, should be among the most important documents. In order to create an effective IS policy, it is necessary to describe correctly and fully the organisation's business environment from the IS viewpoint. Thus, the main aim of this section is to introduce some necessary terms and concepts as well as a special wording for describing unsecure ITI's state in terms of possible IS incidents, which should be detected and avoided in the future.

Standards which were used in Section 1 are ISO/IEC standards from the 27000 series, namely ISO/IEC 27000:2018 (Overview and vocabulary) [ISO/IEC, 27000], ISO/IEC 27001:2013 (Requirements for IS management systems) [ISO/IEC, 27001], ISO/IEC 27002:2013 (Code of practice for IS controls) [ISO/IEC, 27002], ISO/IEC 27005:2018 (IS risk management) [ISO/IEC, 27005], ISO/IEC 27033-1:2015 (Network security -- Part 1: Overview and concepts) [ISO/IEC, 27033-1], ISO/IEC 27033-2:2012 (Part 2: Guidelines for the design and implementation of network security) [ISO/IEC, 27033-2], ISO/IEC 27033-3:2010 (Part 3: Reference networking scenarios -- Threats, design techniques and control issues») [ISO/IEC, 27033-3], ISO/IEC 27032:2012 (Guidelines for cybersecurity) [ISO/IEC, 27032], ISO/IEC 27035-1:2016 (IS incident management -- Part 1: Principles of incident management) [ISO/IEC, 27035-1], ISO/IEC 27035-2:2016 (Part 2: Guidelines to plan and prepare for incident response) [ISO/IEC, 27035-2], ISO/IEC 27043:2015 (Incident investigation principles and processes) [ISO/IEC, 27043] and NIST SP 800-61 Rev. 2 (Computer Security Incident Handling Guide) [NIST, 800-61].

2.1 IS terminology and IS concept

In this subsection, the main terms used in the research are introduced based on [P04]. Many existing IS-related definitions can be accepted in terms of practice, but they do not reflect

specifics of modern information society and require their alignment with the current scientific views. That is why the own definitions are proposed and explained. The glossary proposed contains the following basic terms:

- IS (briefly a quality/property of information to maintain its confidentiality, integrity, availability, authenticity, accountability, non-repudiation, and reliability);
- IS maintenance (in Russian IS maintenance is a broader term in comparison with IS management, to which it adds information protection tools – IPTs [Zapechnikov, 2008]);
- IS management (a cyclic process, consisting of a set of targeted actions taken to achieve organisation's business objectives by ensuring the security of its information sphere and including IS awareness, training, and motivation of employees, posing the IS aim, assessing IS risks and planning their treatment measures, design, implementation and evaluation of the effectiveness of appropriate IS controls, IS roles and responsibilities, and selection of corrective and managed actions and their implementation);
- IS risk (is associated with the potential that IS threats will exploit vulnerabilities of an information asset/group of assets and thereby cause harm to an organisation);
- IS threat ((short from a threat of IS violation) a set of conditions and factors that create an actual or potential opportunity for violation of ITI's IS);
- Source/actor of IS threat (a person, a material object or a physical event, realising an IS threat);
- Vulnerabilities (the IT assets' properties (including IPTs) exploited by IS threat sources for IS threats' realisation);
- Intruder (an entity/subject that implements IS threats to IT assets, using their vulnerabilities and disrupting the authority given to him/her for access or control them);
- Attack (any intruder's action leading to IS threat's implementation via vulnerabilities exploitation. It is the actual violation of IS with the aim to destroy, expose, alter, disable, steal or gain unauthorised access to or make unauthorised use of an IT asset);
- Network security (a secure (protected) state of a computer network infrastructure integrally and all its separate connections and resources, which is provided by means of preventative IS controls, from unwanted IS events).

After that, another group of very important for our research terms, which are discussed in detail in [P01] and completely coincide with ISO/IEC 27000:2018 [ISO/IEC, 27000] are introduced: IS event (an identified/observed occurrence of a system, service or network state indicating a negative consequence such as a possible breach of IS policy or failure of controls, or a previously unknown situation that may be security relevant), IS incident (single or a series of unwanted or unexpected IS events that have a significant probability of compromising business operations and threatening IS), ISIM and ISIM system. IS events can be considered as a part of one IS incident, while the IS incident can be a set of IS events. Any attack on a network is an IS event or incident, depending on an organisation's IS policy.

2.2 IS threats, vulnerabilities, attacks and incidents taxonomy

Using all these definitions and analysing real-world attacks (like Advanced Persistent Threats (APTs), phishing e-mails, pharming, scams, Nigerian spam, Denial-of-service (DoS) attacks, Cross-Site Scripting (XSS), SQL injections, targeted watering hole attacks, ransomware, Heartbleed, ShellShock, Poodle, Gotofail, BadUSB and many others [Zapechnikov, 2006]) and numerous reports of well-known companies (like Symantec, PricewaterhouseCoopers, Endescan, CA technologies, Flexera, etc.), the own taxonomy with four classifications of network vulnerabilities, IS threats, attacks, and incidents is proposed [P07], [P12].

The main classification parameters defined are the following:

- For a vulnerability: its origin sources, risk level (criticality, severity), allocation in ITI, 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.

As an example, the remote attacks taxonomy is shown here (Table 2) [P12].

Table 2. Remote Attacks Taxonomy

Classification parameter	***Parameter's content***
Type	Accomplished (duration), in progress, attempt, suspected.
	Origin nature: malicious or accidental.
Attack started…	From the Internet/Intranet/Extranet, Cloud (public/private), Workstation, Mobile device, USB flash drive, website, etc.
Start conditions	On request from a victim (e.g. MitM).
	On a particular event (e.g. replay attack, spoofing).
	Unconditionally (e.g. sniffing, phishing, flooding).
Malefactors	Criminal, user, administrator, manager, developer, etc.
Motivation	Enrichment, revenge, hacktivism, vengeance, self-assertion, sabotage, espionage, vandalism, etc.
Realized by…	People, software, hardware, process, data, etc.
Influence type	Passive (e.g. sniffing/eavesdropping).
	Active (DoS, spoofing, MitM, flooding, etc.).
Aim – Violation of	Physical integrity – destruction (distortion).
	Logical structure – distortion of the structure.
	Content – unauthorised modification.
	Confidentiality – unauthorised obtaining.
	Property rights – misappropriation of rights.
	Availability – disconnection, destruction.
	Privacy (Personally Identifiable Information (PII) theft).
Victim-Attacker	In one network segment (e.g. sniffing, spoofing).
	In different segments (e.g. DoS, MitM, flooding).
Number of victims/ attackers	Traditional – one attacker to one/many victims.
	Distributed – many attackers to one/many victims.
Feedback with a victim	With a feedback (e.g. spoofing, MitM).
	Without a feedback (e.g. sniffing).
Affected objects	Network & its elements (peripheral device, gateway, channel, subnetwork, etc.), account, information, IPT, service delivery, business/management/technological process, database management system, operating system, file, etc.
Affected information	General/special purpose control & management information, billing information, PII, reference/service/operating/telecommunication environment information,

	etc.
ISO/OSI implementation level	Physical (lock picking, hardware modification, wiretapping, stealing data, etc).
	Data link (ARP cache poisoning, DHCP starvation, MAC modification, wireless client de-authentication).
	Network (spoofing, ICMP flooding, Wormhole/Blackhole attacks, Route cache poisoning).
	Transport (session hijacking, TCP port scan/host sweeps, UDP flooding, etc.).
	Session, Presentation & Application (flooding, viruses, MiTM, repudiation, buffer overflow, DDoS).
	Combined (DDoS, jamming, hijacking, etc.).
Method/ Actions	Ready-to-use Exploit, Brute Force, Improper Usage/Illegal Activities, Scanning & Probing, Masquerading, Counterfeiting, Modification, Copying, Deleting, Sniffing, Flooding, Replacement, Spoofing, MiTM, Pharming, Spamming, Phishing, SQL injection, XSS, CSRF, Email attachment, Ransomware, APT, etc.
Tools	Information interchange, social engineering, hardware, user's commands, software (including toolkits/rootkits, scripts), virus, worm, anonymising proxy, capture, etc.
Damage	Physical harm to people, prolonged downtime, damage to equipment, software and hardware failures, resource theft, IS policies breach, etc.
Damage severity	Minimum, medium, high or critical.
Vulnerability (-ies) used	Lack of IS knowledge/IPTs, poor IS policy, IS policy violation, bad configuration, etc.
IPTs disruption	None, failure, unavailability of critical information to perform functions, violation of IPT's software/hardware integrity, IPT's settings change, etc.
Detection complexity	Normal or high.
Probability of recurrence	Minimum, medium, high or critical.

The proposed taxonomy in comparison to existing ones, for example, the ATT&CK framework by MITRE [https://attack.mitre.org/], is essentially broader in classification parameters used, as the MITRE's matrix presents adversaries' tactics and techniques that corresponds only to one row of the taxonomy (namely the "Method/Actions" row).

Of course, the given taxonomy does not claim completeness, as new IS threats, vulnerabilities, attacks, and incidents are detected almost every day [Katsikas, 2008]. It should be borne in mind that the parameters of classifications should be interrelated in a complex manner. For example, the IS threats sources and the form of their implementation determine the possibility of forming a plurality of the IS threats origin nature and vice versa.

2.3 Key signs of remote network attacks and their implementation as IS incidents

To continue, the most important 28 verbal descriptions of the signs of remote attacks, better known as Indicators of Compromise (IoCs), were worked out [P05], [P12]. They are related to the typical activities or their combination associated with a specific remote network attack, for example:

- Unauthorised user on the network or shared credentials;
- Unauthorised access to confidential data, Personally Identifiable Information (PII) and financial data;
- Unauthorised internal host (client or server) connection to the Internet;
- Excessive access from single or multiple internal hosts to external malicious website (from the known blacklists);
- Off-hour (at night or 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;
- The hosts, which are publicly accessible or allocate in the organisation's network demilitarised zone (DMZ) [Syngress, 2003], communicate to some internal hosts that indicates leapfrogging from the outside to the inside and back, data exfiltration and remote access to the network resources, etc.

The list proposed is not ranked and any organisation can do its own attack prioritisation according their IoCs.

2.4 Specifications unifying the information formats applicable to IS incident description

From our taxonomy, it is obvious that IS incidents can be described in completely different ways. That is why there are many standards (as listed in [P14]), which are designed for unifying these descriptions. Among the most known are the following data exchange specifications:

Incident Object Description and Exchange Format (IODEF) and Real-time Internetwork Defense (RID) by the MILE working group; Intrusion Detection Message Exchange Format (IDMEF) and IODEF for Structured Cybersecurity Information (IODEF-SCI) by IETF; Collective Intelligence Framework (CIF) by REN-ISAC; Vocabulary for Event Recording and Incident Sharing (VERIS) by Verizon; Open Indicators of Compromise (OpenIOC) by Mandiant; Open Threat Exchange (OTX) by Alien Vault; Cyber Observable eXpression (CybOX), Trusted Automated eXchange of Indicator Information (TAXII) and Structured Threat Information Expression (STIX) by MITRE. These standards can be used in our research to form a unified template for IS incident description to be used in NSICs and SIEM 3.0 systems.

2.5 Summary

The international standards, as well as proposed terminology and taxonomy, are useful for any organisation while designing its ISIM system and processes and writing internal documentation for their support as a framework for further extension and refinement. Know more about unsecure network operations, attackers and attack scenarios is essential to better protect organisations' ITI. Here «unsecure» means that only negative elements influencing secure vital data processing and network functioning are considered: vulnerabilities exploited by IS threats for implementation as peculiar attacks, being estimated by organisations as IS incidents. The right choice of adequate IS controls will depend on the completeness and quality of IS policies as well IS threat and intruder models.

Summing up, *the main contributions of Section 2 to the research* are the following:

- Selection of normative base (as a collection of ISO standards) and development of glossary of the research area;
- Development of taxonomy of network vulnerabilities, IS threats, attacks and IS incidents;
- Description of key verbal indicators of IS incidents in networks;
- Selection of specifications for information formats applicable to IS incident description.

In the next section, the glossary proposed, the normative base selected, the taxonomy of network vulnerabilities, IS threats, attacks and IS incidents, as well as the key verbal indicators and

specifications for describing IS incidents in networks are used to discuss an IS incident management process with its subprocesses.

3 IS incident management (ISIM)

Based on the results of the previous section, the ISIM process (ISIMP) is defined with special attention to IS monitoring in it, show what IS-related data should be managed in ISIM and approve that it can be characterised as a big data. Discussion on Security Information and Event Management (SIEM) systems as a core tool for ISIM concludes the section.

3.1 ISIM process and subprocesses

According to ISO/IEC 27035-1:2016 [ISO/IEC, 27035-1], ISO/IEC 27035-2:2016 [ISO/IEC, 27035-2] and NIST SP 800-61 (Rev. 2) [NIST, 800-61], it is essential for any organisation serious about IS to have an effective ISIMP in place as a basic part of the general IS management processes and a structured and planned approach to detect, report, assess, and respond to IS incidents, including the activation of appropriate IS controls to prevent, reduce, and recover from impacts; report vulnerabilities, so they can be assessed and dealt with appropriately; and learn from IS incidents and vulnerabilities, institute preventive controls, and make improvements to the overall approach to ISIM.

Hence, according to the above standards, ISIMP [Miloslavskaya et. al, 2014] contains seven subprocesses (Fig. 3) [P01]:

1) Vulnerabilities, IS events and incidents (VEI) detection;
2) VEI notification;
3) VEI messages processing;
4) IS incident response;
5) IS incident analysis;
6) IS incident investigation;
7) IS incident management process efficiency analysis.

In [P01], the “VEI detection and notification” joint subprocess for some organisation as an example is considered in detail. All employees of the organisation, contractors, and users from

external organisations, using IT systems and services of this organisation, participate in this process. After collecting any information on IS event or IS incident or detecting the suspicious situation, causing suspicion on IS incident or ITI's vulnerability presence, everyone is obliged to inform on the given event an authorised party via predefined in advance communications. The diagram of the developed subprocess is depicted in Fig. 4. The subprocess description, input and output data as well as all processes from Fig. 4 are given in [P01].

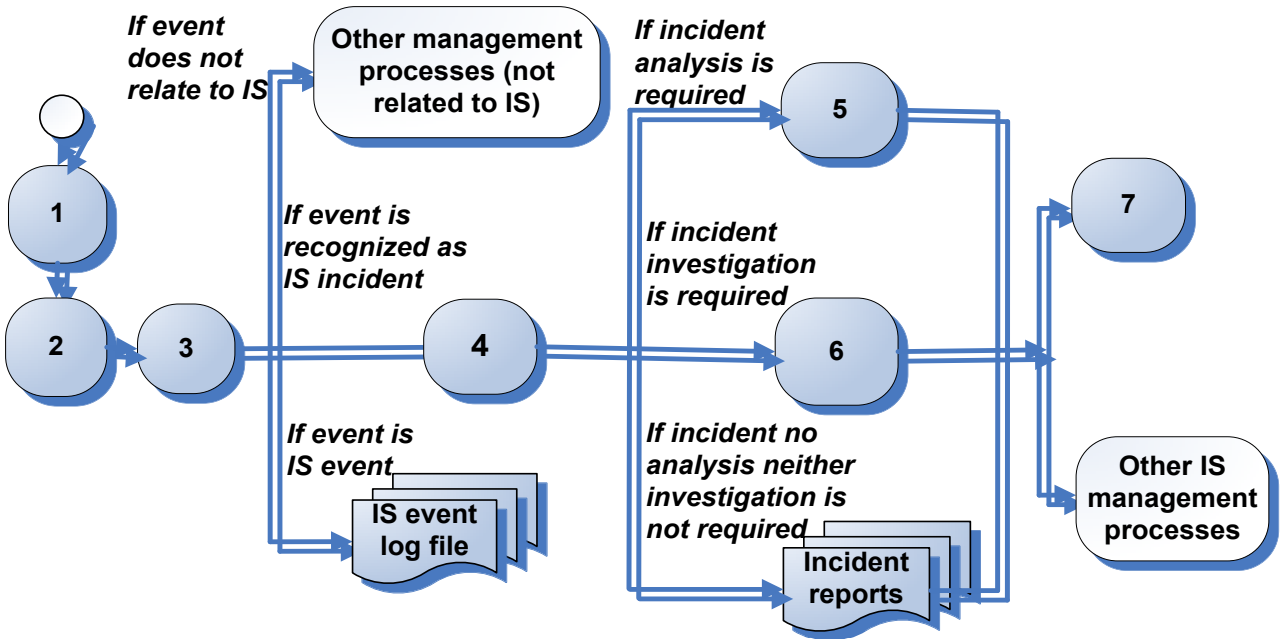


Figure 3. The ISIMP diagram [P01]

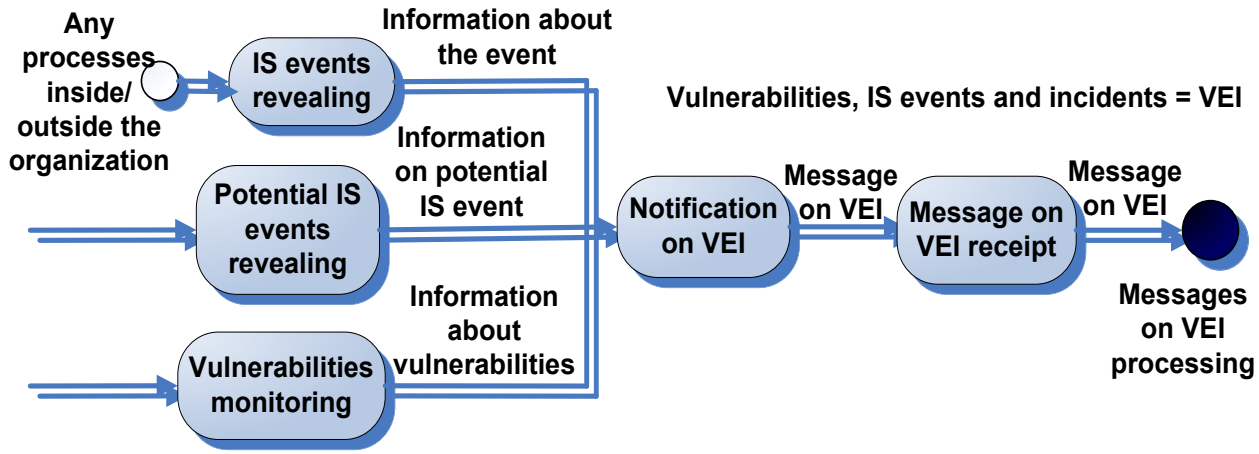
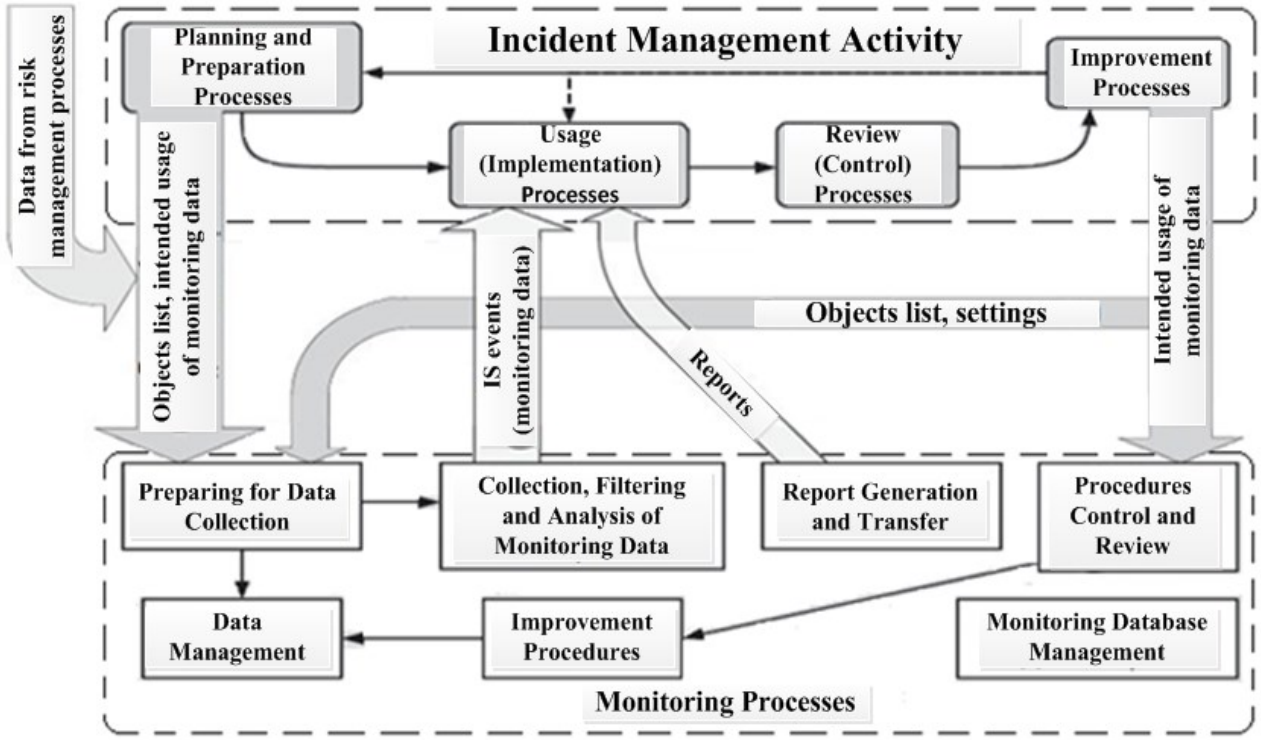


Figure 4. "Vulnerabilities, IS events and incidents detection and notification" joint subprocess diagram [P01]

3.2 Role of IS monitoring in ISIM

Initial data for all ISIMP subprocesses can be collected during different IS checks, including IS monitoring and control of security measures used (collectively called IS monitoring) ([Bejtlich, 2005-1], [Bejtlich, 2005-2] and [Fry, 2009]). In the research, IS monitoring is understood as permanent (continuous) elicitation of events to be registered as affecting organisation's IS maintenance in a particular environment (IT, system, network, service), as well as the collection, analysis and generalisation of the monitoring results. IS monitoring is implemented on the basis of monitoring compliance with the basic requirements for IS maintenance and appointed regulations (control over the normal mode of the environment's functioning) [P02], [Miloslavskaya et al., V5]. Timely provision of the authorised parties with full and reliable information for justified decision-making in the sphere of IS maintenance is one of the main objectives of IS monitoring. Among other tasks, IS monitoring pursues the following purposes: recognition of the contingencies, including malicious, with the organisation's ITI assets and business processes; detection of IS events, partly classified further as IS incidents; detection of the ITI assets' vulnerabilities that attackers can use to implement their attacks; providing evidence in case of computer crimes investigation, etc. IS monitoring also promotes the sense of responsibility in organisation's employees for the actions affecting the IS, helps in detecting misuse of ITI resources and acts as a deterrent for people who can try to harm the organisation.

Preparing for data collection and collection itself, filtering and analysis of the collected data, data management, etc. are the IS monitoring subprocesses, which are associated closely with the ISIM (Fig. 5) [P02], [Miloslavskaya et al., V5]. IS monitoring data is used directly for the ISIM, when IS events are distinguished from all the information observed after primary treatment according to the established criteria. Further, a part of these events will be classified as IS incidents requiring mandatory registration, determination of their causes, detailed study of the essence of what has happened and implementation of an appropriate reaction and elimination of their consequences. In turn, effective ISIM provides rapid restoration of normal ITI functioning, minimises their adverse impact on the organisation's business and prevents their possible occurrence in the future by selecting and implementing adequate IS controls to the problems identified (IS threats and vulnerabilities).



– management flow; ⇨ – data flow

Figure 5. IS monitoring and IS incident management processes interrelation [P02]

After first processing, the collected data are transferred into useful for decision-making information and at the highest level of abstraction, after more complicated processing and understanding, into new knowledge needed not only for tactical but what is more important strategic improvement of an organisation's business [P13] (here in the research, the ideas of Russell Ackoff [Ackoff, 1989], a systems theorist and professor of organisational change, is followed completely).

3.3 IS-related data to be managed in ISIM

All the IS-related data should not be considered as a simple combination of separate data elements [P13]. It is a must to maintain the recorded relationships of every file execution and modification, registry modification, network connection, executed binary in an organisation's environment, etc. Moreover, it is a data stream with the following unique features: huge or possibly infinite volume, dynamically changing, flowing in and out in a fixed order, demanding fast (often real-time) response time, etc.

Typical examples of data streams include various kinds of time-series data and data produced in dynamic intranets such as network traffic (consisting from network packets which are specific for a concrete network protocol), telecommunications, video surveillance, Website click streams, sensor networks, etc.

From IS viewpoint, these heterogeneous data exist in four types of silos:

- Data locked up in disparate security devices and IPTs;
- data collected from scattered applications, etc., creating another silo like another database where that data is stored with no communication and coordination with the first one;
- Data in streams;
- Data segregated by the organisation's business units and operations groups.

For example, the main sources of data on IS events in intranets are the following:

- Log files of IS monitoring systems [Techtarget, 2016];
- System log files of operating systems (OSs) and database management systems (DBMSs); log files of application software, active network equipment and IPTs;
- Network traffic;
- Data from physical access control devices, etc.

The list of very important for ISIM information, which can be filtered from the log files, is given in [P13].

3.4 Application of big data, fast data and data lakes to IS-related data

Thus, in this research big IS-related data IT refers to data-centric/data-driven IT, aimed at processing very large-scale arrays of semi-structured IS-related data in real-time [P03]. Big data is considered primarily as continuous flowing substance, processing mechanisms for which must be built in the streams themselves. Wherein a downstream rate for data incoming for processing and a rate of results delivery should be no lower than the stream rate, as otherwise, this would lead to an infinite growth or queues or useless storage of infinitely increasing volumes of raw data. Data mining ([Han & Kamber, 2006] and [Dua & Du, 2011]) for new IS-related knowledge discovery

consists of the iterative sequence of data cleaning, integration, selection and mining, pattern evaluation, knowledge representation (Fig. 6) [Dua & Du, 2011]. All these steps are discussed in detail in [P03] and they are logically tied to the ideas from [P13].

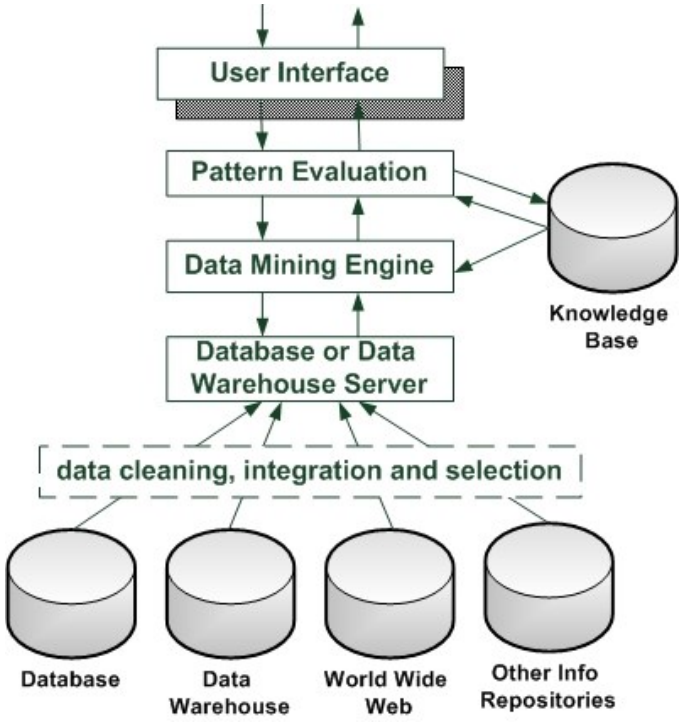


Figure 6. Data mining process for IS-related knowledge discovery [Dua & Du, 2011]

In [P06], another two modern concepts are added to big data. A data lake [Inmon, 2016] for the ISIM purposes refers to a massively scalable storage repository that holds a vast amount of raw IS-related data in its native format ("as is") until it is needed plus processing systems (engine), which can ingest data without compromising the data structure. The goal of fast data analytics [Shalom, 2014] is to gather quickly and mine structured and unstructured IS-related data from thousands to millions of devices so that action can be taken.

3.5 Security Information and Event Management (SIEM) system as a core tool for ISIM

In the conclusion of Section 3, it should be emphasized that IPTs can register millions of IS events of different origins and consequences in the intranets of the large organisation during just one day. The amount of work required to identify the truly important data from the viewpoint of IS events and to obtain information on IS incidents can be extremely large. This complicated and

time-consuming activity can overwhelm the most experienced professionals. The automated systems for ISIM – SIEM systems ([Miller et. al., 2010] and [Scarfone, 2018]) – are used to solve the problem of flow control over the IS events to computerise ISIMP [P10]. These systems are crucial for organisations' IS as they collect logs and other IS-related information for further analysis. They need SIEM systems for compliance purposes to automatically generate reports that provide evidence of organisations' adherence to various compliance requirements. To completely and correctly perform assigned tasks, SIEM systems require frequent tuning and customization as they serve in a constantly changing, dynamic environment.

Therefore, SIEM systems can help to achieve the following objectives in ITI's IS management [P10], [P14]: to obtain information about the real state of the ITI's IS level; to conduct a reasonable assessment of IS risks and timely eliminate or reduce IS risks based on this assessment; to detect differences and bring the ITI assets and business processes in accordance with the internal IS policies, requirements of regulators and auditors; and to formalise and implement effective decision-making in the field of IS.

Typical SIEM system's architecture is depicted in Fig. 7 [IBM, 2010]. The bottom of the figure shows the basic event collection and record retention capabilities. This retained data in the middle is then used for monitoring and correlation tasks. The top shows that the analysed data can be reported in either security information or event-driven reports.

SIEM systems of two generations are known [Chuvakin, 2012]. The first-generation systems of the late 1990's were log-centric and detected IS events through preset rules and information correlation techniques, which were implemented mostly for IP addresses, although some advanced systems could correlate ports and protocols and even users. They used relational databases (DBs), which have the following limitations: little semantic richness and very simple structures, no support for recursion and inheritance, lack of processing/triggers, etc. They could not help to detect the specific client's or malware's activity with context, the use of unauthorised tools like Tor, SSL usage over unusual ports, non-standard network traffic, protocol anomalies, unauthorised connections and so on. These and other shortcomings have spurred the creation of the second-generation SIEM systems (SIEM 2.0) in the late 2000's [Q1 Labs, 2011].

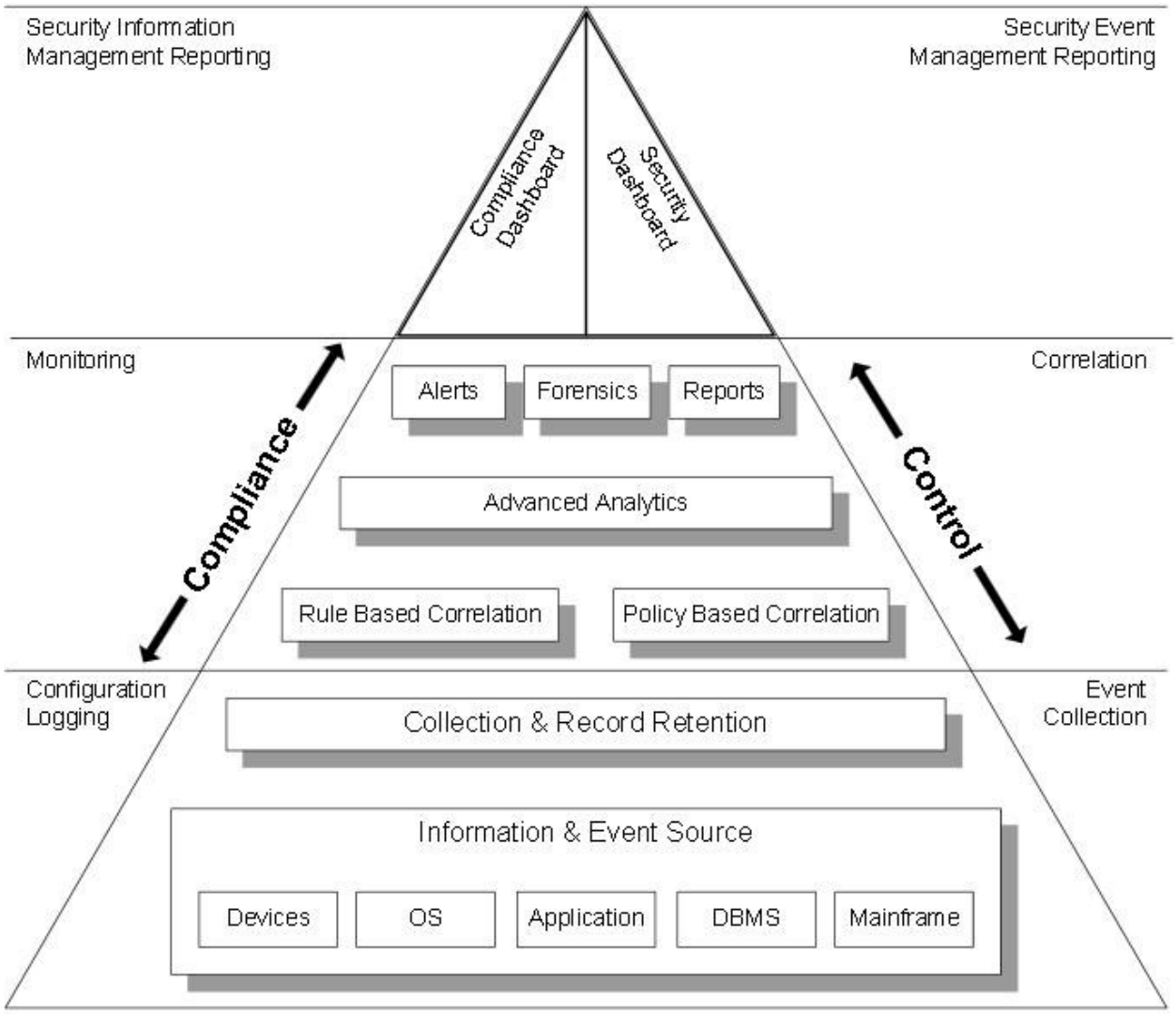


Figure 7. Typical SIEM system's architecture [IBM, 2010]

SIEM 2.0 systems perform behavioural and contextual analysis and implement the following functions: real-time detection and centralised collection of information about IS events from all distributed heterogeneous ITI sources; collected information processing in a particular context, given previous and current user's and application's activity and accumulated statistics; tracking the entire lifecycle of each IS incident, including automatic execution of certain actions in response to IS events classified as IS incidents; automated generation of reports and recommendations to handle IS incidents and events; and big data technologies usage for scalable IS analytics.

3.6 Summary

This section shows that ISIMP is one of the key management processes of any organisation. The data received as the output of ISIMP is the input for another IS management processes and vice versa. For example, IS monitoring gives a lot of interesting information for ISIMP. ISIMP is associated with the processing of large amounts of data, which requires a mandatory automation of routine operations. Properly designed and operating ISIMP reduces the number of IS incidents, limits damage caused by them and can be automated. SIEM systems, being used for the constant events and monitoring users' activities, can detect and handle IS incidents through aggregation of large volumes of machine data in real time for IS risk management, and essentially improve this automation. SIEM systems can also visualise IS threats to organisations' ITIs. From the other side, all SIEM data should be protected itself as it contains sensitive information for digital forensics [Prosise, 2003]. While being integrated with another IPTs, SIEM systems can serve as a single window into IS incidents. That is why they are considered as a core of SOCs and NSICs described further.

Summing up, *the main contributions of Section 3 to the research* are the following:

- Description of seven subprocesses of ISIM process, which are developed in detail by using special notations;
- Demonstration that IS monitoring in the form of VEI detection as one of the important ISIM subprocesses;
- Highlighting the issues of managing big IS-related data during ISIM;
- Identifying SIEM systems' role in ISIM, their functions, and evolution.

In the next section, having all these in mind a Security Operations Centre (SOC) will be presented as a specialised organisation's network unit implementing all the listed above contributions of Section 3.

4 Mission of Security Operations Centres (SOCs) in IS monitoring

We face today many challenges in heterogeneous, complicated and highly distributed ITIs that will continue and tangle in the future. Two important sources of complexity are the vast quantity and variety of security alarms detected and reported by IPTs and the diversity of tasks performed by IS department including management of assets, risks, IPTs, patching, IS incidents, encryption, etc. A single firewall and intrusion detection/prevention system can produce over gigabytes of log data and over millions of messages daily. A part of the information from IPTs is dominated by false positives. Most of the messages are artefacts of the legitimate resources' usage. The task is to isolate and to prioritise a few messages that do indeed indicate IS incidents from the white noise of IPTs' messages [P05], [P08], [P13].

4.1 SOC with SIEM 1.0 system for IS incident monitoring

The key to a more effective automation of security operations workload and prioritisation of the ISIM tasks before ITI may be compromised lies in setting up an in-house specialised unit called a SOC ([Bidou, 2005], [Lukatskiy, 2005], [Romanov, 2005]). The SOC refers to a centralised unit that deals with IS issues on an organisational level plus a team, which is composed primarily of security analysts (and a few operators) organised to detect, analyse, respond to, report on, and prevent IS incidents. The SOC eliminates the need to manually search, gather, evaluate, categorise, analyse and ultimately identify IS-related information from multiple sources. It monitors networks security and can be regarded as a nucleus of network security operations (as a main ITI's part). In most cases with a SIEM 1.0 system as a core, the SOC as a shared ISIM service centre collects data from hundreds of IPTs and builds a picture of ITI's network security health. The key functions of the SIEM 1.0 system in SOCs are log collection, normalisation, correlation, aggregation, and reporting. Its output gives information for an instant response to critical issues and vulnerabilities.

In ITIs SOCs work in a round-the-clock mode and performs the following typical functions [P05]: SOC's operational support system, ITI's asset tracking and recovery, vulnerability scanning followed by patch management, traffic sniffing, device configuration management, centralised

IPTs' management, IS risk management, security information management, IS events/incidents handling, including a local in-house ISIRT (IS incident response team))[Killcrece, 2003], [West-Brown et al., 2003] and [Alberts et al., 2004]), and data and computer forensics. These functions are supported by different extracting, filtering, normalisation, categorisation, correlation and the other analysis techniques and heuristics to determine which malicious IP addresses, Uniform Resource Locators (URLs), applications or something else could harm ITI's resources and to understand which ITI assets' vulnerabilities are most often exploited by attackers.

4.2 SOC types

In [P05], a classification of SOCs is proposed according to the following criteria:

- Counteraction capabilities (SOC without such a capability and reactionary SOC, deployment scenarios (centralised or distributed);
- Aim (controlling/management/crisis);
- Correlation technique (statistical, rule-based, vulnerability, Service Level Agreement (SLA), compliance, mixed, without correlation);
- Implementation variant (software/hardware/infrastructure solution);
- Ownership (in-house/outsourced).

The given classification does not claim completeness and may be broadened if necessary. In addition to it in [Zimmerman, 2014], a special class called Cybersecurity Operations Centre is mentioned.

The SOC's effectiveness is reasonable measured by how IS incidents are managed, handled, administered, remediated, and isolated [P05]. Figuratively speaking any SOC is the ISIM's eyes.

4.3 SOC limitations

The traditional SOCs with outdated rule-based SIEM systems have done well several years ago while protecting against traditional attacks. Nowadays the attack landscape is characterised by more targeted, smarter, stealthier and sophisticated techniques (like APTs and client-side

attacks), and SIEM 1.0 systems cannot cope with the increasing volumes of IS-related data and does not manage to keep control of the situation. Based on the thorough analysis of many sources, the following serious limitations of SOCs were defined [P08], [P13]:

- Inability to work in the large-scale, globally deployed, heterogeneous, highly distributed ITIs with connect-from-anywhere-and-anytime users;
- Incapability of providing a high degree of trustworthiness/resilience in IS event collection, dissemination, and processing, thus becoming susceptible to attacks on the SIEM systems themselves and the entire SOC;
- Dependency on centralised correlation rules processed on a single node, making scalability difficult, and creating a single point of failure;
- Limited IS analysis and assessment capabilities with limited-visibility solutions as SOC monitors above all network-level events and provide not very complicated triage and troubleshooting for ITI;
- A reactive security posture, lack of online reaction to identified attacks and limited threat blocking; hence, SOC's analysts additionally to automated operations should assess real-time IS data and manually respond to it;
- Insufficient capacity to process large volumes of all gathered and analytically derived IS-related data known as big data;
- Inability to interpret data from the higher layers like services;
- A great number of false positives and false negatives, as the SOCs' main application area is uncovering known or easy-to-detect IS threats;
- The old-practice SIEM 1.0 systems used;
- Manual integration of IS ensuring technologies used.

4.4 Summary

Concluding this section, the urgent and immutable modern requirements to the next-generation IS management units are full-visibility, behaviour-based (detecting anomalies from a baseline of normal activity) approaches implementation and a heightened level of ITI's security that brings new IS ensuring technologies with their actionable and comprehensive insight and predictive knowledge management to the forefront.

Summing up, *the main contributions of Section 4 to the research* are the following:

- Analysis of typical SOC's functions in IS monitoring and revealing of their limitations in the current network environment;
- Classification of SOCs.

In the next section, a new evolutionary after SOCs type of centres – Security Intelligence Centres (SICs) are described with an additional contribution of this research in their development.

5 Mission of Security Intelligence Centres (SICs) in IS management

To automate to the limit all routine security operations and IS incident response that does not require experts' decision-making is an urgent need for any modern organisation to set up more advanced ISIM centre than a traditional SOC [P13]. Hence in the section, the vision of the Security Intelligence (SI) concept, which can be used in the research for a NSIC's development as one of the basic concepts, is explained. In the analysis of the evolution of network security ensuring approaches in [P11], it was shown that the era of SI has come since 2010 after perimeter defence (2000-2004) and logging and compliance approaches (2005-2009).

5.1 SI concept and SIC with SIEM 2.0 system for IS management

Until today there is no well-established definition of SI. In the framework of the research, the following one is preferable: SI "is the real-time collection, normalisation, and analysis of the data generated by users, applications and infrastructure that impacts the IT security and risk posture of an enterprise" [Burnham, 2011].

The SI concept emphasizes the need not just to collect IS-related data but to learn from it in order to permanently stay ahead of the intruders. Viewing time-stamped historical data or logs is very important for IS incident investigation but to stop it is possible only when you have a real-time view in a concrete context of what is happening across the entire network right now to find something unusual. Another definition stresses that "Intelligence-driven computer network defence is a risk management strategy that addresses the threat component of risk, incorporating analysis of adversaries, their capabilities, objectives, doctrine and limitations" [Hutchins et. al., 2013]. Put simply, SI's goal is to provide proactive, predictive (forward-looking), actionable and comprehensive protection and insight into network security that reduces IS risks and operational effort for any organisation through advanced analytics [Q1 Labs, 2012].

The following main advantages of the SI concept for ANALYSE & REACT mission in real-time IS incident management are defined as follows in [P13]:

- 24x7 security coverage, combining local monitoring observations, external SI and internal threat intelligence in one place without requiring full-time staffing;
- A holistic approach, meaning that an organisation is looking at every aspect of its IS threat management in relation to every other aspect, views IS as more than a matter of mitigating IS risk by identifying and patching vulnerabilities on network assets, as well as considering IS threat capabilities and motives against ITI's assets;
- A more focused approach, concentrating its resources on concrete IS threats with prioritising the redundant multiple layers of IS that constitute borrowed from the Defense-in-Depth (Castle) strategies and strategically orchestrating these layers;
- Alignment of IS risk management with business needs and qualified IS risk ranking based on BIA (including the relevance of IS threats to specific assets with their value, vulnerabilities, patching levels, countermeasures, as well as suspicious activities, etc.);
- Built-in IS risk framework, vulnerability assessment, patch management, compliance and audit functions, and integrated change control functions;
- The better understanding of overall exposure supported by cross-channel visibility in a single view and entity link analysis to reveal hidden relationships and suspicious associations among users, accounts or other entities early in their life cycles;
- Proactive and predictive monitoring of IS threats (not only activity monitoring), based on predefined meaningful IS metrics for making faster, more-informed, smarter decisions through real-time integration;
- Advanced context-based analytics meaning the ability to correlate observed applications, host and user activities, their geo-location, network traffic telemetry, events and so on with the system, application, network, server, IPT and other logs with patterns and trends in a consistent way (not event-by-event analysis);
- Automated correction of IS problems, white/blacklisting, IPTs alerts, updates and configuration changes, IS incidents escalation and closure as instructed or required;
- Behavioural-based cross-correlation that triggers priority alerts and automated responses based on IS risk scores tied to specific services and combinations of events or thresholds of changes in these indicators;
- Baseline-driven anomaly detection based on atypical actions — once "normal" is defined, "abnormal" events are given heightened visibility;

- Hunting both past and present IS threats based on a continuously recorded history — not just individual events;
- The inclusion of external IS threat feeds (from open, private or commercial sources, such as IP/domain name reputation and block lists, structured and unstructured reports, emails from sharing groups, etc.) enhances the internally sourced behavioural and baseline detection methods;
- A comprehensive reporting dashboard that is aligned with IS metrics;
- Increasing efficiency (in terms of reducing costs and complexity of IS incident response and improving attacks detection accuracy by instantly understanding the entire attack stages chain) via launching a unified defence against IS threats based on centralised case management, a common repository for cross-channel data and shared workflow tools;
- An organisation's network is very often not an intruder's target; contrariwise, the target is the endpoint because the valuable data very often resides there; etc.

After a thorough analysis of the SI concept its main characteristics can be summarised [P11]:

- Objective: log management, application/user activity monitoring, IS threat detection, IS risk management, compliance;
- Architecture: single console and deeper network flow analytics, less intrusive and separated from the data centre;
- Data sources: all relevant IS-related data across the entire organisation's intranet;
- Number of devices managed, events per second, storage: unlimited, based on unique scaling requirements of each deployment;
- Analytics: advanced analytics including all network events, network, application, and user context;
- End users: IT security and compliance teams, operators, auditors, analysts;
- Breach response: real-time/near-real-time discovery of breaches, often with same-day remediation;
- Major limitations: standards governing bodies not yet formed and integration with third-party products/sources still labour intensive.

The SI concept is implemented in SICs with their integrated attack defence architecture, full visibility and context-driven control over network security in one place to deal with higher-level IS events [Lockheed, 2015]. Implementing SICs, organisations get a holistic in-depth view of their ITI's IS health and are capable not only to detect attacks but effectively predict IS threats and prevent IS incidents before they cause harm, constantly producing new knowledge on network attacks and vulnerabilities. Figuratively speaking, the SIC is the IS management's brain with wide-open eyes [P13].

As a truly integrated and multi-domain solution, the SIC combines a number of technologies [P08], [P13]:

- IS knowledge management, promoting an integrated approach to identifying, capturing, evaluating, retrieving and sharing this knowledge;
- Big IS-related data processing;
- ITI asset identification, tracking, and recovery after different IS incidents;
- Data collection capabilities and compliance benefits of log management;
- Centralisation and aggregation of data from disparate silos with ensuing correlation, normalisation, categorisation and analysis by SIEM 2.0 systems;
- Network visibility and advanced IS threat detection of IDS/IPSs for network behaviour (rule-less) anomaly detection;
- IS risk management reducing the number of IS incidents and ensuring compliance;
- IS incident handling, consisting of detection, alerting and notification, reporting, response and escalation management;
- Vulnerability scanning followed by device configuration and patch management;
- Network traffic sniffing and application content insight afforded by Next-Generation FireWalls (NGFWs) and forensic tools.

SIEM 2.0 systems are built as a data store for high-velocity input. They are becoming more scalable and advanced with cross-correlation engines, as well as accelerated and streamlined investigation workflows and big data analytics to support IS events detection, insightful analysis, and forensics into the overall data. These systems tuning for adapting to a particular organisation's changing environment is a foundation for SICs, based on their following capabilities [P10]:

- Fully integrated and centralised log and event management with scale-out architecture for complete situational awareness and robust unified knowledge base, including, inter alia, relevant internal historical data and data from external sources;
- Scalable, multi-dimensional IS-related big data with advanced correlation and pattern recognition, automated behavioural white-listing and statistical base-lining, configuration and patch management, deep packet (searching packet payload for protocol noncompliance, viruses, spam, spyware, network attacks, information leakage and so on) and flow inspection, etc.;
- Extended organisation-wide network security visibility and context, using hosts' activity and file integrity monitoring;
- Logical group analytics which is applied to services, and ITI assets for issue prioritisation, continuous asset profiling and impact analysis;
- Predictive, actionable, intelligent, behaviour- and process-driven response to all IS events with proactive alerting, real-time documenting and reporting and in many products agent-less direct "device-IPT" communication to improve on-line detection, investigation, and remediation;
- Automated compliance and audit assurance for broad IS controls verification and IS policies violations;
- Simplified, ease-of-use management and rich visualisation, based on interactive OSI/ISO layer-2/3 topology and service mapping, as well as various dashboards with built-in rules, reports and widgets;
- The low number of false positives and negatives;
- Prompt and efficient computer forensics with fully-recognized digital evidence.

It was already mentioned that SICs are the next evolution step after SOCs. SOCs' business logic, described by R.Bidou [Bidou, 2005], contains five operational layers and corresponding modules (Fig. 7):

- IS event-based and status-based message generators (like application, servers, services, perimeter and boundary points, internal resources, etc.) (depicted as E Boxes);
- IS-related data acquisition layer on the basis of SIEM with IS event collectors (C Boxes);
- formatted and aggregated IS-related message DB (D Box);
- IS incident analysis engine (A Box) and knowledge base (K Box);

- IS reporting and reaction management software (R Box).

5.2 SIC's business logics

Based on the above analysis of SIC's objectives and outcomes, in the framework of the research it is proposed to extend the given picture by two additional types of boxes (Fig. 8): U and TPI (where ND – a network device, AP – an application, DS – a data stream) [P11].

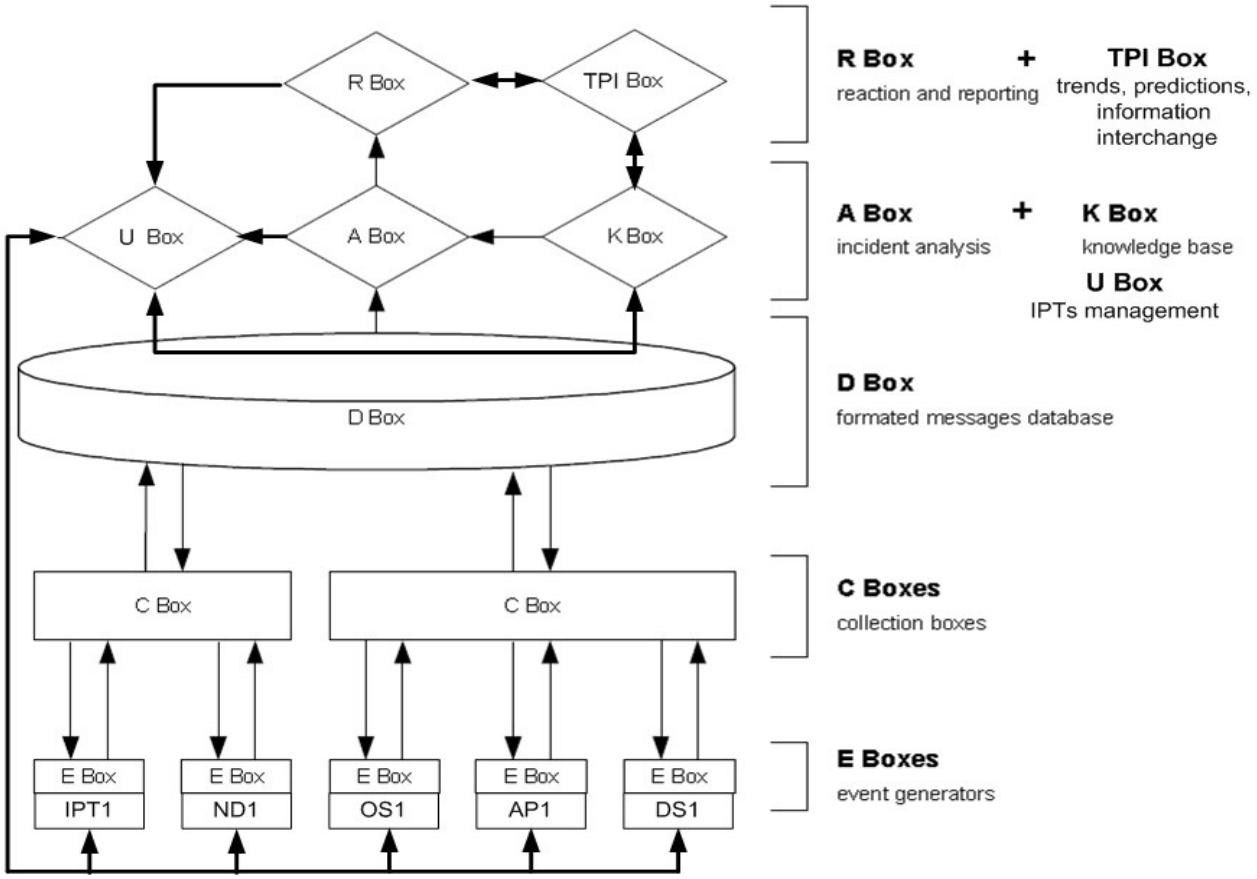


Figure 8. SIC's business logics [P11]

The goal of U Box can be defined as to manage IPTs, including the periodical collection of configuration files from IPTs and their storage in K Box, IPT's configuration change tracking, managing IPT's configuration file versioning, IPT's access accounts storage, and obtaining a set of commands from K Box or directly through the U Box's interface for alteration of IPTs' setups. U Box can be considered as a service. It has the ability to initiate itself the execution of some

commands. Then this would map to an automated response to IS incidents. IPT configuration's change also maps to changes in monitoring.

The goal of TPI Boxes is to manage IS trends (concerning attacks, vulnerabilities, IS threats and incidents), predictions (in a particular environment based on IS trends and its historical data) and IS information interchange and sharing with other parties or unified databases (such as trusted external threat intelligence sources).

In SIC's business logic, TPI Boxes should be connected with two types of boxes:

1) directly with R Boxes for reaction activation (in SICs these actions can be both reactive like in SOCs and proactive), and via them indirectly with U Boxes for rapid IPTs' reconfiguring;

2) directly with K boxes for mining data and creating new knowledge, and via them indirectly with A boxes for more comprehensive analysis.

IS-related data comes into SIC's data systems in streams, and its processing should be implemented as the processing of big data streams at speed. Then IS-related data requires two technologies: a streaming system capable of delivering events as fast as they come in and a data store capable of processing each item as fast as it arrives [P13]. That is why the following requirements for fast IS-related data processing in SICs should be met:

- "Ingest": get millions of events per second, which after processing can be regarded further as IS incidents;
- "Decide": make a data-driven decision on each event potentially influencing network security;
- "Analyse in real time": enable automated decision-making and provide visibility into operational trends of IS threats, vulnerabilities, etc.

Further a multilevel hierarchy of D Boxes can be introduced that will reduce the database query processing time due to the smaller amount of data at the lower. In the longer term the picture can be added by processing another mentioned above IS-related data on IS events, not only configuration files from IPTs.

5.3 SIC's data architecture and big data processing in SICs

For big IS-related data processing in SICs, the more advanced than a big data IT called "data lakes" [Inmon, 2016] is proposed to be used [P11]. The data lake uses a massively scalable storage repository, which holds a vast amount of raw data in its native format ("as is") until it is needed, and appropriate processing systems (engine), which can ingest data without compromising the data structure. The lakes are typically built to handle large, quickly arriving volumes of unstructured data (in contrast to data warehouses processing highly structured data [Inmon & Linstedt, 2014]), from which further insights are derived. Besides, the lakes use dynamic (not pre-build static) analytical applications, which can exploit static, dynamic or both types of data. The data in the lake becomes accessible as soon as it is created (in contrast to data warehouses designed for slowly changing data) that is very important for real-time IS decision-making.

Based on Fig. 8, the SIC's data architecture proposed is an implementation of D Boxes together with the realisation of other boxes on their top. Here the data lake also plays the role of K Boxes. But the architecture in Fig. 9 [P11] is quite simplified and just indicates how big data IT could be used in a small part of the SIC.

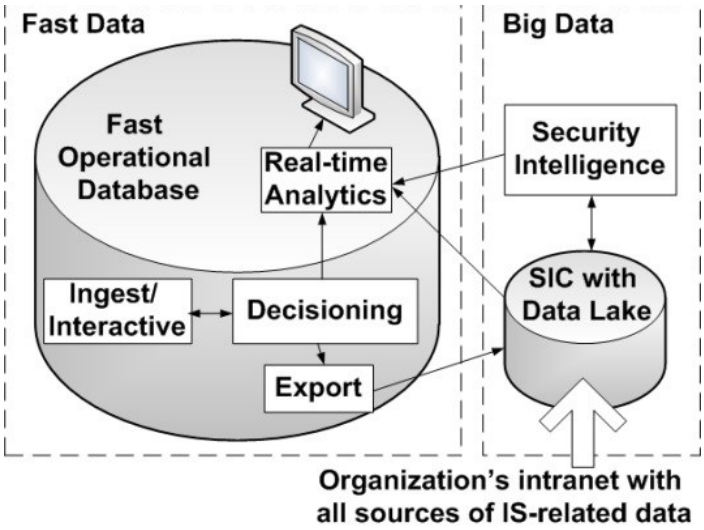


Figure 9. Simplified SIC's data architecture [P11]

The SIC's data lakes should be integrated with the rest of the organisation's ITI, well-managed and protected, have scale-out architectures with high availability, centralised cataloguing and indexing, shared access from any permitted modern device, use agile analytics

and advanced data lineage (tracking). The data going into a lake contain logs (e.g., from the OSs, applications, IPTs) and sensor data (e.g., from the Internet of Things), low-level customer behaviour (e.g., Website click streams), social media, document collections of (e.g., e-mail and customer files), geo-location trails, images, video and audio and another data useful for integrated analysis.

As all IS-related data can be regarded as fast data, it requires immediate processing in order to infer respective events that can lead to the activation of the execution of particular IS controls. The fast data is time-sensitive structured and unstructured "in-flight" data, which should be gathered and acted upon right away (requires low latency and processing of data streams at speed [Marz & Warren, 2013]). It corresponds to the application of big data analytics to smaller data sets in near-real/real-time in order to solve a particular problem. Technologies, which can support real-time analytics in SICs, include processing in memory, in-database or in-memory analytics, data warehouse appliances, massively parallel programming, and others.

5.4 Summary

In comparison with IS controls used in SOC, the new SIC concept logically develops its features to overcome the limitations found.

Summing up, *the main contributions of Section 5 to the research* are the following:

- A generalised description of the SI concept as a logical continuation of IS ensuring approaches, its main advantages and characteristics;
- SICs' function and technologies combined;
- SIEM 2.0 systems' mission in SICs;
- SIC's business logics proposed;
- Simplified SIC's data architecture.

But 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. The next evolutionary step towards the creation of more effective IS management structure for securing organisations' ITI assets is extremely needed. This progressive structure 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. In the next section, a new NSIC's concept as a combination of a SIC and a Network Operations Centre (NOC) is proposed.

6 Network Security Intelligence Centres (NSICs)

In this section, the main results of the research are presented and discussed: the new NSIC's concept as a combination of a SIC and a NOC, the methodology of NSIC's development, its implementation in specialised NSIC with a layered infrastructure and a zone security infrastructure and some issues, the solution of which supports its operations (for example, network security information to be visualised in NSICs, blockchain-based SIEM 3.0 system for NSICs and training of highly qualified staff for NSICs).

6.1 Requirements for NSICs

Considering the limitations of SOCs and SICs and understanding their reasons to eliminate them in new NSICs, the main requirements for NSIC's operation were formulated. Their fulfilment in NSICs is intended to increase the effectiveness, scalability and maintainability of ISIM processes for modern organisations to be proactive and resilient to damaging IS threats as their urgent and priority need. The main specific requirements, which should be taken into account in designing NSICs, can be formulated as follows [P15]:

- All NSIC' processes should be in line to industry regulations and applicable standards (like ISO/IEC 27000 series);
- Usage of more types of data for analytics: there is still a lack of skills and techniques how to process unstructured data-at-rest, RAM data from endpoints, data from mobile endpoints, virtual and cloud environments;
- Modular and adaptive IS event management achieved by using modular and configurable IPTs and network devices, measures, functions, and protocols, concentrating all IS management processes to be reused by different NSICs;
- Operational resilience (the ability to adapt to changing patterns and to alter operations in face of changing business conditions) against targeted attacks on the NSIC itself and faults of incremental severity, ensuring long-term permanent availability, integrity and confidentiality and another properties (like accuracy, reliability, etc.) of the information

flows, their dissemination infrastructure, crucial processing units, knowledge and DBs, etc. It eliminates a single point of failure and includes software and hardware stability;

- Scalability (the ability to increase or decrease in performance and cost in response to changes in application and system processing demands) in terms of scalable data acquisition and collection of vast amounts of events from diverse internal/external sources forming all together big IS-related data;
- Elasticity (the ability of a system to increase the workload on its current and additional (dynamically and automatically added on demand) computing resources over time) for distributed and near real-time aggregation, dissemination, and processing of hybrid big IS-related data, combining batch and stream data processing;
- Agility as getting needed SI tools in hands so the NSIC's staff can interrogate all currently available data and get results from different points of view;
- Maintainability with centralised architecture and distributed operation of its separate business processes, combining scalability and elasticity of data collection, storage, pre-processing and correlation across integrated and distributed/decentralised implementation as a response to the changing environment and new IS threats;
- The NSIC's security and trustworthy, including its infrastructure and processes security, as well as big IS-related data security and trustworthy (trusted governed data come from trusted sources). Additionally, it is necessary to protect big data processing processes themselves, as well as all their inputs and outputs.

6.2 NSIC as a combination of a SIC and a NOC

As the SIC has been already described in Section 5, NOCs are briefly explained further. They are typically owned by large organisations (of course, outsourcing is possible, but it is out of the scope of our research). Their main goal is to support a centralised place, from which network administrators can supervise, maintain and monitor their telecommunications networks via all necessary software to manage optimal network operations across a variety of platforms, mediums and communication channels, and to visualize their detailed status with all individual devices being monitored [P15]. NOCs achieve this goal by executing a set of checks and recovery procedures for critical data, applications, and networks. They can be considered as a focal point for the following NOCs' staff typical activities [Continuum, NS]:

- Network discovery, assessments, management, continuous support of high availability;
- Performance monitoring, reporting, improvement recommendations and tracking problems until they are resolved;
- Constant research of anomalies and troubleshooting to deliver critical alerts to the right personnel, isolate problems, identify root causes, marshal resources, automatically escalate urgent issues, etc.;
- Management of domain names, configurations, releases, storage, emails, voice and video traffic, end-users' support, etc.;
- Systems' administration and backup;
- Optimisation and quality of service management, prevention of services' degradation;
- Application software installations, distribution, troubleshooting and updating;
- Policy enforcement and SLA management;
- Coordination with affiliated networks;
- Elementary IS controls like authentication and authorisation, IP- and MAC-address filtering; etc.

A unified NSIC as a combination of SIC and NOC is proposed. Its main goal is to move intelligence-driven IS to organisations' NOCs, which allows staying ahead of IS challenges in an increasingly online world while being fully integrated around key business processes [P15]. To implement migration to NSIC is possible because both SIC's and NOC's operation functions are frequently organised in a similar way, which is based on a tiered approach with similar roles at the lowest levels and share some instrumental tools at the technical layer. Their union would be beneficial in a long-term perspective as the NOC's primary concern is serving the business, while the SIC's main focus is to ensure its security. When an outage is detected, NOC's personnel is likely to attribute the disruption to devices' malfunction or systems' issue and attempt to address it through hardware replacement or configuration adjustment. In addition, the SIC's personnel are likely to attribute the problem to malicious activity and will thus prompt an investigation before initiating the appropriate IS event response actions.

Hence, the NSIC introduces powerful synergies of SICs and NOCs via people collaboration and toolkits and techniques joint usage. Significant benefits of NSICs to their owners are the following [P15]:

- Complete situational awareness with seamless integration of the monitored entities from network and SI services with a supporting infrastructure including monitoring and IPTs;
- Network and security real-time monitoring, meeting IS management requirements and including network performance and availability automated monitoring, alerting and notification (based on network management protocols), standard client/server protocols, SLA reporting, link usage, integrated service desk, etc.;
- Centralised network devices' and IPTs' configuration management and audit, including changes mapped to IS controls' change and rollback, baseline configuration violations, a complete history of changed configurations and so on;
- Network devices change management in place with the automated approval process, links to configuration templates, change control validation and history log;
- Computer-based data collection and analytics from both network and IS viewpoints to extract maximum value from the massive amounts of IS-related data available in NSICs;
- Monitoring of all network activity linked to identities as opposed to IP addresses;
- IPTs alerts' prioritisation according to the most likely events that can result in most negative impacts;
- Richer organisation-wide context mining to aid operational and strategic IS decision-making and to validate that the right IS policies are in place;
- Ability to provide, record and frequently update metadata for each detected IS event/incident for its recursive analysis. This metadata is critically important for SI in order to minimise data noise and to differentiate events and incidents from each other;
- Faster IS event detection and reduced IS incident response times by automated remediation and enabling IS controls and IT to work together, with each contributing specialised functions, skills, and experiences;
- Advanced network forensics including a full packet capture, user's sessions reconstruction, integration with IS incident response handling, etc.;
- Improved countermeasure planning and implementation through joint accountability for identification and resolution of root causes;
- Actionable streamlined ISIM (including behavioural analytics for continuous monitoring, pre and post analysis) and reporting with valuable context;

- The centralised management console for dashboards and reporting, IS risk and compliance management, network topology mapping and visualisation;
- Regular IS audit and assessment with IS metrics reporting and executive summary;
- Improved communications with predetermined escalation and effective knowledge sharing to enhance situational awareness and coordinate response capabilities;
- Measurement of Key Performance Indicators (KPIs) based on performance monitoring and false negatives/positives, reducing "IS event signal-to-noise" ratio.

Based on NSIC's objectives and intended functioning outcomes, four key NSIC's business processes are identified:

1) Network security monitoring, audit, and assessment;
2) Event classification and triage;
3) Prioritization, analysis and prediction;
4) Remediation and recovery.

The more integrated and automated the SIC-NOC interaction, the more effective the whole NSIC will be. Again, figuratively speaking the NSIC is an IS management's rapid brain with wide-open eyes and skilful hands [P15]. However, the operating models and processes of only leading organisations are sufficiently mature to support this advanced joint model of proactive operation built on a big data processing architecture.

6.3 Network security information to be visualised in NSICs

Considering a separate IS event, it is proposed to visualise for decision-making in NSICs the following information [P02]: 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. For example, log files contain important information, which can be visualised:

- User's (access subject) identifier;
- Dates and times of his log-ins/log-outs, details of the events;
- Information about the host, which initiated the event to be registered and/or its location;
- Records of successful/rejected attempts to access the objects;
- Changes in systems' configurations;
- Modified lists of access subjects and objects;
- Changes in access subjects' authorities and access objects' status;
- All privileged actions (using the supervisor account, running and stopping the system, connecting/disconnecting to the input/output devices);
- Starting programs and processes, which accessed protected objects;
- Usage of system utilities and applications;
- Established sessions;
- Files which have been accessed, and the type of access;
- Network addresses and protocols;
- Changes in the intensity and volume of incoming/outgoing traffic;
- Printing materials containing sensitive information;
- Access to critical systems and services;
- Systems' warnings and failures;
- Alarm raised by the access control system and IDS;
- Changes or attempts to change settings and tools for system protection management;
- Activation/deactivation of IPTs;
- The appearance of new devices with uncontrolled access, etc.

6.4 The methodology of NSIC development

Organisations are expected to follow the traditional in that case step-by-step methodology for NSIC establishing, implementation, maintenance, and continuous improvement, described by

the well-known Deming-Shewhart Wheel or PDCA/PDSA cycle [Techtarget, 2015]. For the NSIC, these steps are recommended as follows [P16].

Step 1. PLAN and strategize: Settle on an agreement of the NSIC's vision that is in line with the organisation's business goals, and integrate this vision with its business plans. Define the NSIC via establishing its mission, objectives, responsibility, scope, charter and IS policies in place, and strategy and governance. Establish the resources and budget for the NSIC.

Step 2. DO and develop governance:

2.1. Determine and document the IS management key processes and standard operational procedures required to support by the NSIC for ISIM, at a minimum: network monitoring; compliance monitoring; alerting and notification (email, mobile, chat, etc.); a process and a flow for decision-making and escalation; IS event and IS incident logging, investigation and reporting; dashboard creation; IS incident response; communications; transition of daily services; change management; etc. All processes' organisation and integration issues, as well as the NSIC's zoning (segments) according to the role-based access and data processed should be also solved, etc. All necessary security monitoring tools to collect raw IS-related data should be set up for making sure that the organisation's critical servers, services, and IPTs are all sending their logs and other important data to the NSIC's log management and analytics. Among these tools are those for asset discovery, vulnerability assessment, intrusion detection, behavioural monitoring, and security analytics.

2.2. Staff the NSIC with highly trained personnel from a technical background who understand the real-world impact of IS threats and vulnerabilities and the actual methods hackers use to break into systems (with at least Security Analyst, Security Specialists, Forensics/Threat Investigators) and define their competencies (in terms of knowledge-skills-abilities), training, roles, operational hours and so on.

2.3. Launch the NSIC and manage the IS events complete life cycle (from collecting to removal), including their categorisation, prioritisation, IS incident opening, assignment and closing, and users' errors validation.

2.4. Maintain daily shift operations and IPTs to find suspicious/malicious activity, including, but not limited to the following: analysing alerts and performing triage on them by determining their criticality and scope of impact, evaluating attribution and adversary details, investigating Indicators of Compromise, reviewing and editing event correlation rules, as well as sharing the findings with the threat intelligence community, etc.

2.5. Put and use feedback procedures in place, as well as serve as the initial point of contact for customers on the organisation's ITI.

Step 3. STUDY/CHECK: Perform rudimentary testing, measurement, and diagnosis of ITI, as well as the NSIC's operations monitoring and auditing.

Step 4. ACT: Propose and implement improvements for the NSIC's functioning, process changes/upgrades, etc.

In accordance with these steps of the iterative NSIC's evolution, organisations should determine and provide all necessary resources, including funding, IS policies (e.g., for NSIC's data centre), processes, procedures, IS metrics, services, staffing, communication, etc.

6.5 NSIC's layered infrastructure

Further, based on the best practices of constructing infrastructures for the complicated network systems from the business operations and IS perspective, five NSIC's infrastructural layers can be defined (Fig. 10) [P16].

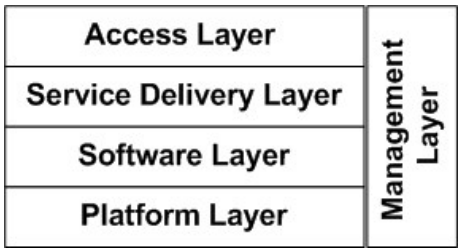


Figure 10. NSIC's layered infrastructure [P16]

The Platform layer provides a set of resilient building blocks (above OS level) for the next Software layer and includes network, storage, backup, virtualisation, computing, and other facilities. Together with the Software layer represents the enabling perspective within Information and Communications Technology (ICT).

The Software layer provides the applications and software, which support all NSIC's business activity and uses application services from the Platform layer.

The Service Delivery layer delivers those NSIC's service management activities that require input and interaction with its service owner. The components are also responsible for the translation of IS management requirement into technology and operational capabilities (like service optimisation, service lifecycle, catalogue and level management, business processes, demand, financial management, etc.). This layer represents the NSIC's business perspective on the basis of ICT.

The Access layer is connected to the Service Delivery and Management layers. The Access layer is where the NSIC's service end users connect to the NSIC. This layer allows to manage and maintain access to the NSIC as a single point using the combination of multiple services through ICT lines and solves the large-capacity, high-performance and high-reliability access problems in the NSIC's devices, network channels, protocols, etc. (for example, via performing load balancing).

The Management layer provides management services and a set of capabilities to the Platform and Software layers via a suite of management tools necessary to support the Service Delivery layer and operational processes carried out by ICT, as well as to support staff in managing networks, services, changes, availability, incidents, problems, knowledge, deployment, provisioning and configuration, monitoring, reporting, systems administration, data protection, etc. The Management layer represents the operational perspective within ICT. Our key proposal for the Management layer is to separate data and management. That will ensure the entire NSIC's management being free of the interference from data, as well as management of the NSIC's Platform and Software layers in real time and protection against attacks.

All these layers and interconnections between them should be protected by the appropriate IS controls. Hence, a secure NSIC's infrastructure should reflect ensuring its IS from different points of view – organisational, technical, hardware, software, etc. All of them deserve a separate and careful consideration. In [P16], the research was briefly focused only on the latter two aspects.

6.6 NSIC's zone security infrastructure

The proper NSIC's security infrastructure, which allows all IS-related data to be collected, indexed, normalised, analysed and shared in a secure way, is required to perform such diverse and extensive work. This infrastructure can be designed according to two possible options: as a built-in secure NSIC within ITI or stand-alone secure NSIC. In both cases, it should be open, flexible, scalable and resilient with well-defined, standardised input and output data formats, high performance and high availability as everyday requirements. And to be truly effective and secure it should have a multi-layered defence, be constantly monitored and well-maintained including operation management, performance and availability monitoring, compliance management, etc.

From our point of view, it is reasonable to apply a zoning design principle with multi-layered segmentation via Firewalls to the NSIC's security infrastructure. Security zone planning is determined by the type of data being processed in a certain zone, the type of access to data and processes in this zone. Security zones are abstract conceptual NSIC infrastructure's dedicated parts with predefined boundaries. These zones are concerned with authorised data flow between them. The resulting NSIC's high-level security zone diagram is depicted in Fig. 11 [P16].

Figure 11. NSIC's high-level zone security infrastructure [P16]

It includes four zones: demilitarized, trusted, restricted and management zones. The Untrusted Zone contains the organisation's ITI network assets not owned by the NSIC and not included in it.

The Demilitarized (Semi-Trusted) Zone is a physical or logical NSIC's forefront subnetwork for external-facing servers and services, which are externally shared by the NSIC and organisation's networks as well as remote and infra NSIC's services (like DNS, SMTP, etc.).

The Trusted Zone with the controlled environment after the internal back-end Firewall is intended for the NSIC's internal-exposed systems (like internal load balancing, device testing and troubleshooting platforms, application services and management, services with limited access to the NSIC's staff only, etc.).

The NSIC's high risk and mission-critical systems (critical services, critical servers, the NSIC's Data Centre, etc.) are allocated in the Restricted Zone.

The Management Zone is created for all NSIC's assets such as infrastructure services, network devices and traffic telemetry, storage and data centre with certain computational power and applications necessary to support NSIC's centralised functioning and accommodate its big data, virtualisation, configuration, changes, patch, backups and NSIC's IS management systems, including IS centralised real-time logging, monitoring, reporting, SIEM system, analytical tools, regulatory compliance, security scanners, etc.

The following main benefits of NSIC's security zone segmentation and management were defined in the research:

- Focus on different IS policy-based protection of NSIC's critical assets according to their location and IS risk assessment and predefined deny rules for all inter-zone connections;
- Strict role-based inter-zone communication access (for both inbound and outbound requests and connections), centralised logging, monitoring and control specified separately for each zone, critical assets' group and a particular asset and user through managed zones' boundaries;

- Special rules for confidentiality and integrity of critical data stored within a zone;
- Ability to detect suspicious activity on the basis of using different IS policy rules for network-based IPS sensors (in network channels) and host-based IPS agents (on hosts) in NSIC's separate security zones;
- Ability to limit IS incidents' impacts using advanced IS analytics, including network behaviour anomaly detection, predictive IS threat modelling, enhanced visibility of IS-related events, traffic, users' activity and assets status in each NSIC's zone;
- Complication of a compromise or virus infection between zones by locking them down to prevent further impacts;
- More opportunities for expedite detection, investigation, response and recovery after IS incidents not reflected in a timely manner;
- All security zones are logically isolated from each other, but transmit all necessary data to each other according to the approved for them IS policies.

6.7 NSIC's implementation in the MEPhI

In [P09] and [P18], the 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 was shared. Its goal was to implement a model of NSIC for its study and continuous improvement.

The NSIC is based on three bearing laboratories with NGWFs, Data Loss Prevention (DLP) and SIEM systems at their cores respectively. At present, it is used only for educational purposes (because the hardware and software base of the centre is still not fully developed for research purposes), which are further discussed in subsection 6.9.

While designing the NSIC, its self-protection was at the main focus [P09], [P18]. Based on a comprehensive analysis of the security level of our department network (investigating logs, using security scanners, etc.), all information resources that are to be protected within the NSIC (using the common approaches of asset inventory and categorisation as the initial steps of IS risk assessment) were defined first. It is typically sensitive data used in a typical network of an educational institution, for example, proprietary information of limited propagation, sensitive

information related to the NSIC's activities, PII of its staff and trainees, learning and testing materials protected by copyright, keys, credentials, passwords, etc. After that two generalised IS models for the NSIC were worked out (the IS threat model and the IS intruder model) and, on this basis, the IS policies were developed, including policies for usage of all applicable IPTs and IS controls; establishing monitoring and auditing policies and procedures; IS event and incident processing; vulnerability management; configuration and changes management; user' s activity registration; filtering of incoming and outgoing traffic; protection against computer viruses and unauthorised software modification and insertion; control over all NSIC's computer port usage; and protection against DoS attacks and unauthorised scanning.

6.8 Blockchain-based SIEM 3.0 system for NSICs

The modern challenge of real-time processing of big IS-related data for justified network security management and the need to secure IS incidents' computer evidence from intruders dictate the need to build these systems using advanced technologies. After careful analysis of the blockchain concept and SIEM systems' evolution, the decision to work out next-generation blockchain-based SIEM 3.0 system was made.

A blockchain-based SIEM 3.0 system for the NSIC as its core was proposed in the framework of the research [P14]. Here a blockchain (BC) refers to a type of secure distributed data structure (DB), which maintains a constantly expanding list of non-editable blocks without any central administrator and data storage and sets rules about transactions. Such a DB is shared by a group of participants, who can submit new blocks for inclusion. One illustration of forming a block for further inclusion in BC is given in [P14] (Fig. 12). Further, the timestamps for the events were also added.

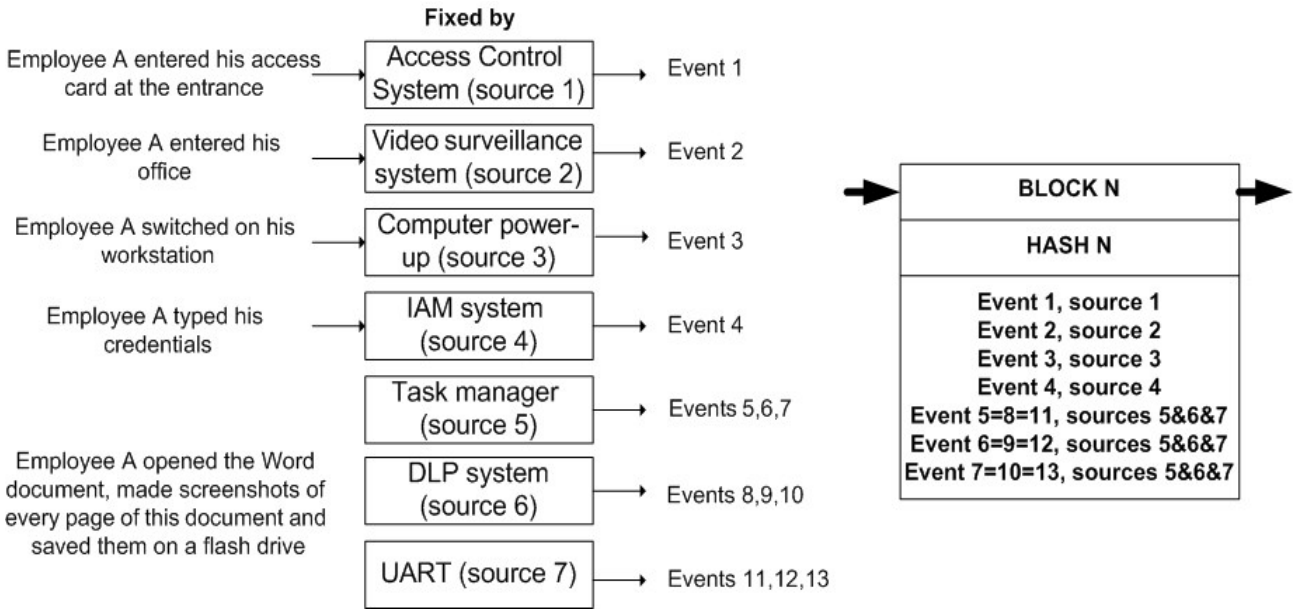


Figure 12. One example of forming a block in the SIEM 3.0 system [P14]

The following BC features can provide significant benefits to our NSIC [P14]:

- BC supports an opportunity to investigate a consequence of IS events leading to an IS incident. By recording every event, it provides a way to use in-depth analysis and check for patterns across thousands of events in real-time;
- BC as a distributed networked system is characterised by interoperability according to applicable international standards, interoperability of data from all sources (data has to have the same syntactic and semantic foundations, which can be developed from unified specifications) and policy interoperability (policies and procedures for data processing need to be aligned);
- A sufficient capability to register, validate, process and transmit to the BC billions of events per second quicker and cheaper, commensurate with normal volumes of collected IS events to meet the needs of the modern network-connected world. Data on each IS event is delivered to BC in hard real-time without any delays. All data is time-stamped and is presented in a structural format for further processing;
- BC is updated automatically every time a new IS event occurs. New blocks with information about new IS events are sent to BC strictly according to the time of their occurrence, one by one;
- The possibility of inserting some additional attributes (e.g., purpose, repeated event, composed of other events, affected asset location) to all data coming to BC to

"colorize" IS events according to their seriousness that will require further mandatory tracking;

- Data integrity for transmissions to, from and within the BC;
- Independence of BC from the type and number of data sources – if they are replaced by new IPTs or their number increases, BC continues to operate;
- Obligatory proof of data source identity and authenticity, to which the parties can trust;
- Real-time event recording with a complete event history supporting traceability and transparency.

The resulting BC-based SIEM 3.0 system's architecture, completely assigned with the SI concept, is depicted in Fig. 13 [P14].

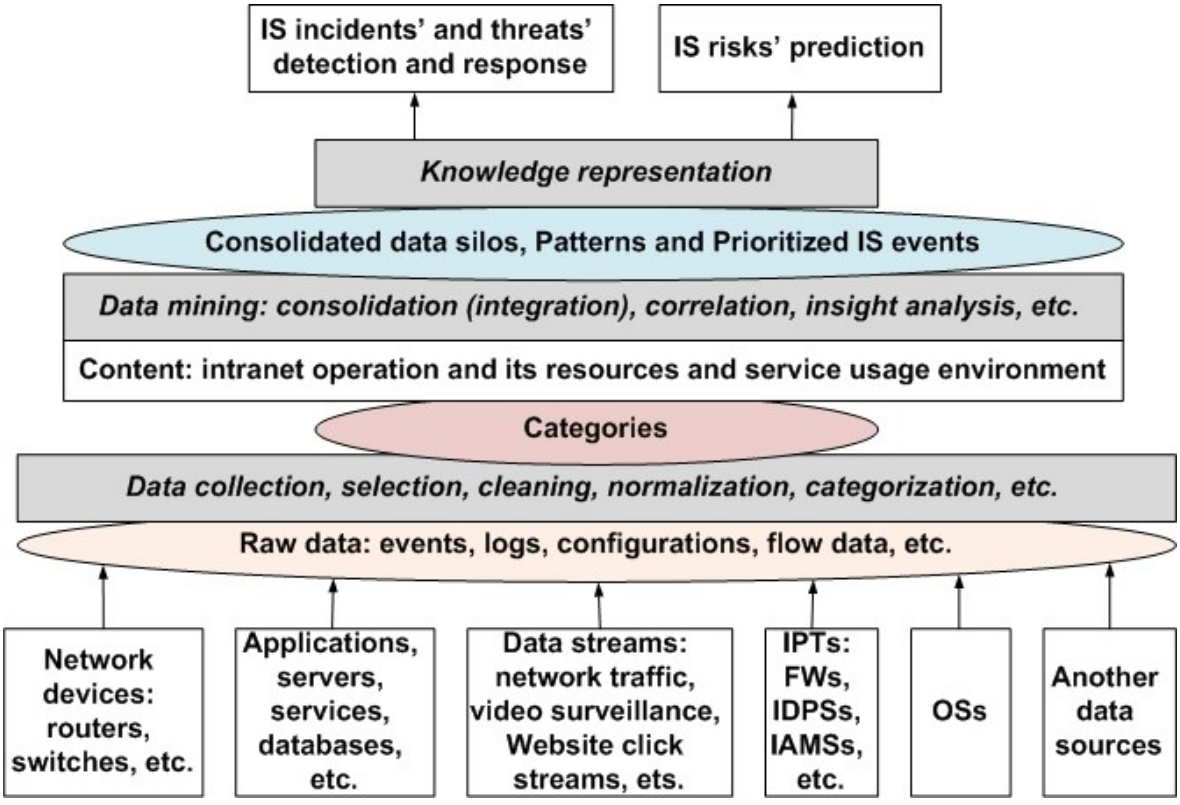


Figure 13. SIEM 3.0 system's architecture [P14]

Even though our system has not been yet implemented, a methodology for validating that the resulting SIEM 3.0 satisfies efficiently and reliable the requirements for SIEM systems is needed in advance to provide in the future a basis for proving that it is realisable, complete,

consistent, unambiguous, and verifiable. For evaluation, modelling of SIEM 3.0 is suggested by using such mathematical objects as sets, relations, functions, which form the basis of all formal languages. One of such well-known possible solutions is the Z notation [ISO/IEC, 13568] used for describing and modelling computing systems (to which SIEM systems can be attributed) via mathematical notation.

6.9 Training of highly qualified staff for NSICs

In the rest of Section 6, the issues of training of highly qualified staff for NSICs are briefly reviewed based on [P09], [P17], [P18] and [P19]. It should be understood that it is a topic for separate research. But it cannot be left without any consideration so far as even in all the related works on SOCs it is noted that their staff is their integral part.

A team of NSIC personnel for 24 x 7 monitoring should be built in a proper way. A professional to work in a NSIC must have specific qualifying characteristics. The modern approach to determining them should be based on the definition of a set of professional competencies demonstrating a professional's capacity to support NSIC's operations and to perform specific work within this sphere of activity. In ISO/IEC 27000:2018 [ISO/IEC, 27000], the following definition can be found: "IS management system professional – a person who establishes, implements, maintains and continuously improves one or more information security management system processes", which is completely applicable to NSICs.

The efforts to develop a common approach to vocational training's Common Body of Knowledge (CBK) (a collection of information and a framework that provides a basis for understanding terms and concepts in a particular knowledge area) and requirements to the IS professional competencies are underway worldwide for a long time. The first attempts to create a common point of view on the subject in general were made at the World International Conferences on IS Education (WISEs) in the late 1990's and early 2000's. About the same time, some CBKs for security professionals were initiated by the industry for certification purposes (like CISA, CISSP, GIAC, etc.).

At present, three main views – American, Australian and European – have been formed [P20]:

- "Information Technology Security Essential Body of Knowledge: A Competency and Functional Framework for IT Security Workforce Development" by the National Cyber Security Division of the U.S. Department of Homeland Security [ITS EBK, 2008] and the more specialised National Initiative for Cybersecurity Education (NICE), led by the National Institute of Standards and Technology [NIST, 800-181];
- "Cyber Security Capability Framework & Mapping of IS Manual Roles" by the Australian Government Information Management Office [CSCF&M, 2010];
- e-Competence Framework 3.0 (e-CF 3.0) by the European Commission [e-CF3.0, 2014].

Recently, the Joint Task Force on Cybersecurity Education (JTF) has successfully developed the Cybersecurity Curricular Guidelines in 2017 [CCG, 2017]. The JTF is a collaboration between major international computing societies: Association for Computing Machinery (ACM), IEEE Computer Society (IEEE CS), Association for Information Systems Special Interest Group on Security (AIS SIGSEC), and International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8).

In the same year the ISO/IEC 27021:2017 standard [ISO/IEC, 27021] on competence requirements for IS management systems professionals has been published. This standard divides the competencies of IS management system professionals into two groups: General or domain-independent, including managerial; and Professional or domain-specific for IS and ISMS Planning – Operation – Support – Performance evaluation – Improvement (particularly for the IS and IS management system areas like Risk Management, Incident Management, Auditing, Security Controls, Business Continuity, Forensics, Access Control, Data Protection, Intrusion Prevention, Vulnerabilities Assessment, Physical and Environmental Security, Cryptography, etc.). NSIC's staff must have all these competencies in volumes, which correspond to their job function.

In respect to the NSIC proposed, the work on launching the "Business Continuity and IS Maintenance" Masters' degree programme in the MEPhI in 2015 should be mentioned [P17]. Among its core educational disciplines are the following: "IS management", "IS risks management", "IS incident management", "IT security assessment", "Business continuity

management", "Protected information systems", "Objects' IS maintenance technologies" and "Confidential data loss prevention".

In support of this programme, various laboratory works, the description of which were presented in detail in a few papers, were worked out. For example, on the basis of the MEPhI's NSIC the following labs are conducted:

- "Study of Next-Generation Firewalls" for the "Objects' IS maintenance technologies" discipline [P09]. To develop students' skills in configuring NGFW settings and customisations, a laboratory bench for testing all basic NGFW functionality during fulfilment of 5 assignments was created;
- "Study of Data Loss Prevention systems" for the "Confidential data loss prevention" [P18]. Five assignments have been developed that allow students to learn how to interact with the DLP system, including configuration of IS event detection policies and information interception rules, generating different reports, conducting IS incident investigations, etc.;
- "Computer Forensics for IS incident investigation" for the "IS incident management" discipline [P19]. After these labs our students will obtain the following basic skills: to organise ISIM, in particular the collection and analysis of IS incident information to decide on a subsequent response; to participate in the design and operation of the organization's ISIM systems; to develop drafts of organisational and administrative documents, as well as technical and operational documentation for ISIM systems; to make a choice and use tools for managing IS incidents. Our labs (with 11 assignments) have one important advantage: they take into account the specifics of IS incidents for Online Banking Services [STO1.3, 2016] as much as possible. The originality of our results is using the scenario of money transfers as a way of engaging students in a specific risk-laden activity performed globally.

6.10 Summary

In this section, only the key ideas of designing the NSIC as a SIC-NOC combination were presented.

Summing up, *the main contributions of Section 6 to the research* are the following:

- Formulation of the modern network environment's requirements for new NSICs;
- Proof that the NSIC proposed as a SIC-NOC combination fully meets these requirements;
- Description of methodology for NSIC's development;
- Definition of network security information to be visualised in NSICs;
- Development of NSIC's layered infrastructure;
- Development of NSIC's zone security infrastructure;
- A brief description of NSIC's implementation in the MEPhI;
- Development of a blockchain-based SIEM 3.0 system for NSICs and its architecture;
- Development of issues for the training of highly qualified staff for NSICs.

In case an organisation already has its own SOC or SIC and made a decision to replace it by the advanced NSIC, NSIC's secure infrastructure can be integrated with the existing SOC/SIC security tools and processes in place initially in parallel to the existing connections (for example, this provision concerns SIEM systems) and finally completely retooling for NSIC's security zones.

In the concluding section, the main contributions of the research are summarized, and some suggestions for future work are made.

7 Conclusion

As stated in the Introduction, the primary purpose of the research was to develop and begin to implement the concept of a new state-of-the-art centralised network security management unit called NSIC. From our viewpoint, the creation of an innovative NSIC concept, its interpretation, construction and initial implementation through original research presented contributes substantially to the modern networks' security, as it extends the forefront of the SOCs and SICc used nowadays and generates significant new knowledge and understanding of network security requirements and solutions. 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 this 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.

7.1 Research Contributions

Summing up, *the main contributions of the research* are the following:

- In Section 2, for forming the basis for the research, the normative base (as a collection of ISO standards) was selected, the glossary of the research area was worked out, the taxonomy of network vulnerabilities, IS threats, attacks and IS incidents was developed, key verbal indicators of IS incidents in networks were described, and specifications for information formats applicable to IS incident description were selected;
- Using the above results, in Section 3, seven subprocesses of ISIM process were developed in detail and described using special notations (namely VEI detection, VEI notification, VEI messages processing, IS incident response, IS incident analysis, IS incident investigation, and ISIM process efficiency analysis), IS monitoring in the form of VEI detection was discussed as one of the important ISIM subprocesses, the issues of managing big IS-related data during ISIM were highlighted, and SIEM systems' role in ISIM, their functions and evolution were identified;

- Further in Section 4, typical SOC's functions in IS monitoring were analysed, classification of SOCs was proposed, and SOCs' limitations in the current network environment were revealed;
- After that in Section 5, following the evolution analysis, a generalised description of the SI concept as a logical continuation of IS ensuring approaches was done, including its main advantages and characteristics, SICs' function and technologies combined were defined, SIEM 2.0 systems' mission in SICs was shown, SIC's business logics was proposed and simplified SIC's data architecture was developed;
- Generalising all the results obtained in Section 6, the modern network environment's requirements for NSICs were formulated, compliance with these requirements of the NSIC as a SIC-NOC combination was proven, NSIC's development methodology was described, network security information to be visualised in NSICs was defined, NSIC's layered infrastructure and zone security infrastructure were proposed, NSIC's implementation in the MEPhI was briefly described, blockchain-based SIEM 3.0 system for NSICs and its architecture were developed, and the most important issues for the training of highly qualified staff for NSICs were discussed.

7.2 Research Results Presentation

The results of the research were published in the following journals:

- Scientific Visualisation (MEPhI, Moscow, 2014, Vol. 6, N 2);
- Journal of Intelligent & Fussy Systems (IOS Press, Netherlands, 2018);
- Information and Computer Security (Emerald Publishing, 2018, Vol. 26, N 4).

The results of the research were presented at the following international conferences:

- The 3rd International Conference on Internet Technologies and Applications (ITA2009);
- The 8th, 10th and 11th World Conferences on Information Security Education (WISE8, WISE10 and WISE11);
- The 1st, 3rd and 4th International Symposiums on Big Data Research and Innovation (BigR&I-2014, BigR&I-2016 and BigR&I-2017);
- The 7th International Conference on Security of Information and Networks (SIN2014);
- The 4th International Conference "Future Internet of Things and Cloud" (FiCloud 2016);

- The 5th World Conference on Information Systems and Technologies (WorldCIST 2017);
- The 8th and 9th Annual International Conferences on Biologically Inspired Cognitive Architectures (BICA 2017 and BICA 2018).

7.3 Future Work

Future plans for the framework include the development and subsequent implementation of educational standards; new programmes/curricula and competency models for different educational levels for specialised network security professional training; supervising Ph.D. students carrying out their research within the NSIC's scope; conducting summer schools with intensive network security programmes, etc. The NSIC can be used to create a trusted educational environment for blended learning with a set of e-learning courses on network security management. And 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, usage of big data technologies for IS-related data processing, the study of the compatibility between different IPTs and recommendations to address arising issues, evaluating network security, etc.

8 References

8.1 Prior Published Works

[P01] Kostina A., Miloslavskaya N., Tolstoy A. Information Security Incident Management. Proceedings of the 3rd International Conference on Internet Technologies and Applications. 8-11 Sept 2009, Wrexham, UK. Pp. 27-34.

[P02] Miloslavskaya N., Tolstoy A., Birjukov A. Information Visualisation in Information Security Management for Enterprises's Information Infrastructure. Scientific Visualisation. Moscow, NRNU MEPhI, 2014. Vol. 6, № 2. Pp. 74-91.

[P03] Miloslavskaya N., Senatorov M., Tolstoy A, Zapechnikov S. Information Security Maintenance Issues for Big Security-Related Data. Proceedings of 2014 International Conference on Future Internet of Things and Cloud FiCloud 2014. International Symposium on Big Data Research and Innovation (BigR&I). 27-29 August 2014, Barcelona (Spain). - C. 361-366. ISBN: 978-1-4799-4357-9/14. DOI: 10.1109/ FiCloud.2014.64.

[P04] Malyuk A., Miloslavskaya N. Information Security Theory Development. Proceedings of the 7th International Conference on Security of Information and Networks (SIN2014), September, 9-11 2014 Glasgow (UK). ACM New York. Pp. 52-55. ISBN: 978-1-4503-3033-6. DOI: 10.1145/2659651.2659659.

[P05] Miloslavskaya N. Security Operations Centers for Information Security Incident Management. Proceedings of the 4th International Conference on Future Internet of Things and Cloud (FiCloud 2016). 22-24 August 2016, Vienna (Austria). Pp. 131-138. DOI: 10.1109/FiCloud.2016.26.

[P06] Miloslavskaya N., Tolstoy A. Application of Big Data, Fast Data and Data Lake Concepts to Information Security Issues. Proceedings of 2016 4th International Conference on Future Internet of Things and Cloud Workshops. The 3rd International Symposium on Big Data Research and Innovation (BigR&I 2016). 22-24 August 2016, Vienna (Austria). Pp. 148-153. DOI: 10.1109/W-FiCloud.2016.41.

[P07] Miloslavskaya N., Tolstoy A., Zapechnikov S. Taxonomy for Unsecure Big Data Processing in Security Operations Centers. Proceedings of 2016 4th International Conference on Future

Internet of Things and Cloud Workshops. The 3rd International Symposium on Big Data Research and Innovation (BigR&I 2016). 22-24 August 2016, Vienna (Austria). Pp. 154-159. DOI: 10.1109/W-FiCloud.2016.42.

[P08] Miloslavskaya N. SOC- and SIC-Based Information Security Monitoring. A. Rocha et al. (eds.), Recent Advances in Information Systems and Technologies, Advances in Intelligent Systems and Computing. Springer International Publishing AG 2017. Vol. 570. Pp. 364-374. DOI 10.1007/978-3-319-56538-5_37.

[P09] Miloslavskaya N., Tolstoy A., Migalin A. “Network Security Intelligence” Educational and Research Center. In: Bishop M., Futcher L., Miloslavskaya N., Theocharidou M. (eds) Information Security Education for a Global Digital Society. WISE 2017. IFIP Advances in Information and Communication Technology. Springer. 2017. Vol. 503. Pp. 157-168. DOI: 10.1007/978-3-319-58553-6_14.

[P10] Miloslavskaya N. Analysis of SIEM Systems and Their Usage in Security Operations and Security Intelligence Centers. 2018. In: Samsonovich A., Klimov V. (eds) Biologically Inspired Cognitive Architectures (BICA) for Young Scientists. BICA 2017. Advances in Intelligent Systems and Computing. Springer, Cham. 2018. Vol 636. Pp. 282-288. DOI: 10.1007/978-3-319-63940-6_40.

[P11] Miloslavskaya N. Security Intelligence Centers for Big Data Processing. Proceedings of 2017 5th International Conference on Future Internet of Things and Cloud Workshops. The 4th International Symposium on Big Data Research and Innovation (BigR&I-2017). 21-23 August 2017, Prague (Czech Republic). Pp. 7-13. DOI 10.1109/W-FiCloud.2017.7.

[P12] Miloslavskaya N. Remote Attacks Taxonomy and their Key Verbal Indicators. Proceedings of the 8th Annual International Conference on Biologically Inspired Cognitive Architectures (BICA 2017). 1-6 August 2017, Moscow (Russia). Procedia Computer Science. 2018. Vol. 123. Pp. 278-284. DOI: 10.1016/j.procs.2018.01.043.

[P13] Miloslavskaya N. Information Security Management in SOCs and SICs. Journal of Intelligent & Fussy Systems. IOS Press. Netherlands. 2018. Vol. 35, N 3, pp. 2637-2647. DOI:10.3233/JIFS-169615.

[P14] Miloslavskaya N. Designing Blockchain-based SIEM 3.0 System. Information and Computer Security. Emerald Publishing. UK. 2018. Vol. 26, Iss. 4, pp. DOI: 10.1108/ICS-10-2017-0075.

[P15] Miloslavskaya N. Network Security Intelligence Center as a Combination of SIC and NOC. Postproceedings of the 9th Annual International Conference on Biologically Inspired

Cognitive Architectures, BICA 2018 (Ninth Annual Meeting of the BICA Society). Procedia Computer Science. 2018. Vol. 145, pp. 354-358. DOI: 10.1016/j.procs.2018.11.084.

[P16] Miloslavskaya N. Developing a Network Security Intelligence Center. Postproceedings of the 9th Annual International Conference on Biologically Inspired Cognitive Architectures, BICA 2018 (Ninth Annual Meeting of the BICA Society). Procedia Computer Science. 2018. Vol. 145, pp. 359-364. DOI: 10.1016/j.procs.2018.11.085.

[P17] Miloslavskaya N., Senatorov M., Tolstoy A., Zapechnikov S. “Business Continuity and Information Security Maintenance" Masters' Training Program. IFIP Advances in Information and Communication Technology. ISBN 978-3-642-39376-1. Ronald C. Dodge Jr., Lynn Futcher (Eds.): Information Assurance and Security Education and Training - 8th IFIP WG 11.8 World Conference on Information Security Education, WISE 8, Auckland, New Sealand, July 8-10, 2013, Proceedings, WISE 7, Lucerne Switzerland, June 9-10, 2011, and WISE 6, Bento Gonçalves, RS, Brasil, July 27-31, 2009, Revised Selected Papers. Springer 2013. Vol. 406. Pp. 95-102. DOI: 10.1007/978-3-642-39377-8_10.

[P18] Miloslavskaya N., Morozov V., Tolstoy A., Khassan D. DLP as an Integral Part of Network Security Intelligence Center. Proceedings of 2017 5th International Conference on Future Internet of Things and Cloud (FiCloud2017). 21-23 August 2017, Prague (Czech Republic). Pp. 297-304. DOI 10.1109/FiCloud.2017.15.

[P19] Miloslavskaya N., Tolstoy A. Developing Hands-On Laboratory Works for the “Information Security Incident Management” Discipline. 2018. In: Drevin L., Theocharidou M. (eds) Information Security Education – Towards a Cybersecure Society. WISE 2018. IFIP Advances in Information and Communication Technology. Springer, Cham. 2018. Vol 531. Pp. 28-39. DOI: 10.1007/978-3-319-99734-6_3.

[P20] Miloslavskaya N., Tolstoy A. State-Level Views on Professional Competencies in the Field of IoT and Cloud Information Security. 2016. Proceedings of 2016 4th International Conference on Future Internet of Things and Cloud Workshops. The 3rd International Symposium on Intercloud and IoT (ICI 2016). 22-24 August 2016, Vienna (Austria). Pp. 83-90. DOI: 10.1109/W-FiCloud.2016.31.

8.2 Additional references

[Ackoff, 1989] Ackoff R.L. From Data to Wisdom, Journal of Applies Systems Analysis, Vol. 16 (1989), pp. 3-9.

[Alberts et al., 2004] Alberts C., Dorofee A., Killcrece G., Ruefle R., Zajicek M. CMU/SEI-2004-TR-015 «Defining Incident Management Processes for CSIRT». October 2004.

[Bejtlich, 2005-1] Bejtlich R. The Tao of Network Security Monitoring: Beyond Intrusion Detection, Boston, MA: Pearson Education, 2005.

[Bejtlich, 2005-2] Bejtlich R. Extrusion Detection: Security Monitoring for Internal Intrusions, Addison-Wesley Professional, 2005.

[Bertalanffy, 1968] Bertalanffy L. von. General System Theory: Foundation develop,emt, Applications. 1968. New York. 289 p.

[Bidou, 2005] Bidou R. Security Operation Center Concepts & Implementation. 2005. Available at: http://iv2-technologies.com/SOCConceptAndImplementation.pdf. Accessed 17.12.2018.

[Burnham, 2011] Burnham J. What Is Security Intelligence and Why Does It Matter Today? August 2011. https://securityintelligence.com/what-is-security-intelligence-and-why-does-it-matter-today/. Accessed 17.12.2018.

[CCG, 2017] Cybersecurity Curricula 2017. Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. A Report in the Computing Curricula Series. ACM/IEEE/AIS SIGSEC/IFIP Joint Task Force on Cybersecurity Education. 2017. Available at: https://www.csec2017.org/. Accessed 17.12.2018.

[Chuvakin, 2012] Chuvakin A. On Large-scale SIEM Architecture. Available at: http://blogs.gartner.com/anton-chuvakin/2012/07/25/on-large-scale-siem-architecture/. Accessed 17.12.2018.

[Continuum, NS] What Is a Network Operations Center (NOC)? Available at: https://www.continuum.net/resources/mspedia/network-operations-center-noc-explained. Accessed 17.12.2018.

[CSCF&M, 2010] The Cyber Security Capability Framework & Mapping of ISM Roles. Final Report. Australian Government Information Management Office. June 2010.

[Dua & Du, 2011] Dua S., Du X. Data Mining and Machine Learning in Cybersecurity. Auerbach Publications. Taylor & Francis Group. 2011. 223 p.

[e-CF3.0, 2014] The European e-Competence Framework 3.0. A common European Framework for ICT Professionals in all industry sectors. CWA 16234:2014 Part 1. CEN.

[Fry, 2009] Fry C., Nystrom M. Security Monitoring, Cambridge: O'Reilly, 2009.

[Hackmaggedon, 2018] Passeri. P. January – September 2018 Cyber Attack Statistics. Hackmaddenon. October 15, 2018. Available at: https://www.hackmageddon.com/2018/10/15/ january-september-2018-cyber-attack-statistics/. Accessed 17.12.2018.

[Han & Kamber, 2006] Han J., Kamber M. Data Mining: Concepts and Techniques. Second Edition. Elsevier. 2006. 743 p.

[Hutchins et. al., 2013] Hutchins E.M., Clopperty M.J., Amin R.M. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Lockheed Martin Corporation, 2013.

[IBM, 2010] IT Security Compliance Management Design Guide with IBM Tivoli Security Information and Event Manager. 2nd edition. Available at: http://www.redbooks.ibm.com/ abstracts/sg247530.html?Open. Accessed 17.12.2018.

[Inmon, 2016] Inmon B. Data Lake Architecture: Designing the Data Lake and Avoiding the Garbage Dump. 2016. 1 edition. Technics Publications. 166 p.

[Inmon & Linstedt, 2014] Inmon W.H., Linstedt D. Data Architecture: A Primer for the Data Scientist: Big Data, Data Warehouse and Data Vault. 2014. 1st Edition. Morhan Kaufmann. 378 p.

[ISO/IEC, 10165-1] ISO/IEC 10165-1:1993 Information technology -- Open Systems Interconnection -- Management Information Services -- Structure of management information: Management Information Model.

[ISO/IEC, 13568] International Organization for Standardization. ISO/IEC 13568:2002/Cor 1:2007 Information technology -- Z formal specification notation -- Syntax, type system and semantics.

[ISO/IEC, 27000] International Organization for Standardization. ISO/IEC 27000:2018 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary.

[ISO/IEC, 27001] International Organization for Standardization. ISO/IEC 27001:2013/Cor 2014, 2015 Information technology -- Security techniques -- Information security management systems – Requirements.

[ISO/IEC, 27002] International Organization for Standardization. ISO/IEC 27002:2013/Cor 2014, 2015 Information technology -- Security techniques -- Code of practice for information security controls.

[ISO/IEC, 27005] International Organization for Standardization. ISO/IEC 27005:2018 Information technology -- Security techniques -- Information security risk management.

[ISO/IEC, 27021] International Organization for Standardization. ISO/IEC 27021:2017 Information technology -- Security techniques -- Competence requirements for information security management systems professionals.

[ISO/IEC, 27032] International Organization for Standardization. ISO/IEC 27032:2012 Information technology -- Security techniques -- Guidelines for cybersecurity.

[ISO/IEC, 27033-1] International Organization for Standardization. ISO/IEC 27033-1:2015 Information technology -- Security techniques – Network security -- Part 1: Overview and concepts.

[ISO/IEC, 27033-2] International Organization for Standardization. ISO/IEC 27033-2:2012 Information technology -- Security techniques – Network security -- Part 2: Guidelines for the design and implementation of network security.

[ISO/IEC, 27033-3] International Organization for Standardization. ISO/IEC 27033-3:2010 Information technology -- Security techniques – Network security -- Part 3: Reference networking scenarios -- Threats, design techniques and control issues».

[ISO/IEC, 27035-1] International Organization for Standardization. ISO/IEC 27035-1:2016 Information technology -- Security techniques -- Information security incident management -- Part 1: Principles of incident management.

[ISO/IEC, 27035-2] International Organization for Standardization. ISO/IEC 27035-2:2016 Information technology -- Security techniques -- Information security incident management – Part2: Guidelines to plan and prepare for incident response.

[ISO/IEC, 27041] International Organization for Standardization. ISO/IEC 27041:2015 Information technology -- Security techniques -- Guidance on assuring suitability and adequacy of incident investigative method.

[ISO/IEC, 27042] International Organization for Standardization. ISO/IEC 27042:2015 Information technology -- Security techniques -- Guidelines for the analysis and interpretation of digital evidence.

[ISO/IEC, 27043] International Organization for Standardization. ISO/IEC 27043:2015 Information technology -- Security techniques -- Incident investigation principles and processes.

[ITS EBK, 2008] Information Technology Security Essential Body of Knowledge: A Competency and Functional Framework for IT Security Workforce Development. September 2008. U.S. Department of Homeland Security. Available at: https://www.hsdl.org/?view&did=234220. Accessed 17.12.2018.

[Katsikas, 2008] Katsikas S.K., Miloslavskaya N. Securing Information and Communications Systems: Principles, Technologies, and Applications. Chapter 8. Network Security. Artech House. 2008. ISBN 13: 978-1-59693-228-9. Pp. 139-170. (Textbook)

[Killcrece, 2003] Killcrece G., Kossakowski K.-P., Ruefle R., Zajicek M. «Organizational Models for Computer Security Incident Response Teams». December 2003. Available at: https://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14099.pdf. Accessed 17.12.2018.

[Lockheed, 2015] SOC vs. SIC: The Difference of an Intelligence Driven Defense® Solution. A White Paper Presented by: Lockheed Martin Corporation. 2015.

[Lukatskiy, 2005] Lukatskiy A. Security Operations Centers. «Information Security» Journal. 2005. Vol. Pp. 28-30. (In Russian)

[Lynch, 2008] Lynch C.A. Big data: How do your data grow? *Nature*, 455, 28-29 (04 September 2008). Available at: https://doi.org/10.1038/455028a. Accessed 17.12.2018.

[Marz & Warren, 2013] Marz N., Warren J. Big Data: Principles and best practices of scalable real-time data systems. Manning Publication Co. 2013, ISBN: 9781617290343.

[Miller et. al., 2010] Miller D., Harris S., Harper A., VanDyke S. Security Information and Event Management (SIEM) Implementation. McGraw-Hill. 2010. 464 p.

[Miloslavskaya et al., 2014] Miloslavskaya N.G., Senatorov M.Y., Tolstoy A.I. «Information Security Management Issues» Series. In 5 volumes. Volume 3: Information Security Incident and Business Continuity Management. Moscow: Goriachaja linia-Telecom. 2014. 2nd edition. 170 p. (In Russian)

[Miloslavskaya et al., V5] Miloslavskaya N.G., Senatorov M.Y., Tolstoy A.I. «Information Security Management Issues» Series. In 5 volumes. Volume 5: Checks and Assessment of Information Security Activity. Moscow: Goriachaja linia-Telecom. 2016. 2nd edition. 166 p. (In Russian)

[NIST, 800-181] Newhouse W., Keith S., Scribner B., Witte G. NIST Special Publication 800-181. National Initiative for Cybersecurity Education (NICE). Cybersecurity Workforce Framework. August 2017. Available at: https://doi.org/10.6028/NIST.SP.800-181. Accessed 17.12.2018.

[NIST, 800-61] Cichonski P., Millar T., Grance T., Scarfone K. NIST SP 800-61 Rev. 2. Computer Security Incident Handling Guide. August 2012. Available at: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf. Accessed 17.12.2018.

[Prosise, 20013] Prosise C., Mandia K., Pepe M. Incident Response and Computer Forensics, Second Edition, McGraw-Hill/Osborne, 2003.

[Q1 Labs, 2011] Evolution of the Modern SIEM. Q1 Labs. 2011. Available at: http://protect.suvo-consulting.de/files/2013/02/SIEM-Evolution.pdf. Accessed 17.12.2018.

[Q1 Labs, 2012] IT Executive Guide to Security Intelligence. Transitioning from Log Management and SIEM to Security Intelligence. Q1 Labs Whitepaper. 2012. Available at: http://www.databreachtoday.com/whitepapers/executive-guide-to-security-intelligence-transitioning-from-siem-to-w-554. Accessed 17.12.2018.

[Romanov, 2005] Romanov V. Operations Centers in Solving Information Security Problems. «Information Security» Journal. 2006. Vol. 3-4. P. 28. (In Russian)

[Scarfone, 2018] Scarfone K. Introduction to SIEM services and products. July 2018. Available at: http://searchsecurity.techtarget.com/feature/Introduction-to-SIEM-services-and-products. Accessed 17.12.2018.

[Shalom, 2014] Shalom N. The next big thing in big data: fast data. 2014. Available at: http://venturebeat.com/2014/06/25/the-next-big-disruption-in-big-data/. Accessed 17.12.2018.

[STO1.3, 2016] Bank of Russia Standard STO BR IBBS-1.3-2016 "Maintenance of Information Security of the Russian Banking System Organizations. Collection and Analysis of Technical Data When Responding to Information Security Incidents during Money Transfer".

[Syngress, 2003] Building DMZs For Enterprise Networks. 2003. Syngress. 767 p.

[Taylor, 1998] Taylor F.W. The Principles of Scientific Management. 1998. Dover Publications. Originally published: New York, Harper & Bros., 1911. 80 p.

[Techtarget, 2015] Techtarget. PDCA (Plan-Do-Check-Act). 2015. http://whatis.techtarget.com/definition/PDCA-plan-do-check-act. Accessed 17.12.2018.

[Techtarget, 2016] Log management. June 2016. Available at: http://whatis.techtarget.com/definition/log-management. Accessed 17.12.2018.

[West-Brown et al., 2003] West-Brown M.J., Stikvoort D., Kossakowski K.-P., Killcrece G., Ruefle R., Zajicekm M. «Handbook for Computer Security Incident Response Teams (CSIRTs),» April 2003. Availanle at: http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6305. Accessed 17.12.2018.

[Zapechnikov, 2006] Zapechnikov S.V., Miloslavskaya N.G., Tolstoy A.I., Ushakov D.V. Information security of open systems. Textbook in 2 volumes: Vol. 1 – Threats, vulnerabilities, attacks and protection approaches. Moscow: Goriachaja linia-Telecom. 2006. 536 p. (In Russian)

[Zapechnikov, 2008] Zapechnikov S.V., Miloslavskaya N.G., Tolstoy A.I., Ushakov D.V. Information security of open systems. Textbook in 2 volumes: Vol. 2 – Network Protection Tools. Moscow: Goriachaja linia-Telecom. 2008. 558 p. (In Russian)

[Zimmerman, 2014] Zimmerman C. Ten Strategies of a World-Class Cybersecurity Operations Center. The MITRE Corporation. 2014. 334 p.

Appendix A - Published Works

Publication 01

Information Security Incident Management

Anna Kostina, Natalia Miloslavskaya and Alexander Tolstoy

Proceedings of the 3rd International Conference on Internet Technologies and Applications. 8-11 Sept 2009, Wrexham, UK.

Abstract

The modern requirements and the best practices in the field of Information Security (IS) Incident Management Process (ISIMP) are analyzed. “IS event” and “IS incident” terms, being used for ISIMP, have been defined. An approach to ISIMP development has been created. According to this approach ISIMP processes are described. As an example the «Vulnerabilities, IS events and incidents detection and notification» joint process is examined in detail.

Research Contribution

This paper explains and defines two main terms used in the ISIM process and subprocesses, namely IS event and IS incident in the framework of ISIM analysis. ISIM process including its seven subprocesses is examined in detail.

N.Miloslavskaya’s contribution: Description of ISIM process as a whole and its subprocesses in a tabular form.

Publication 02

Information Visualisation in Information Security Management for Enterprises's Information Infrastructure

Natalia Miloslavskaya, Alexander Tolstoy and Alexander Birjukov

Scientific Visualisation. Moscow, NRNU MEPhI, 2014. Vol. 6, № 2.

Abstract

The necessity of information visualization on information security (IS) events and incidents originating in an enterprise's information infrastructure (II) is justified. The main IS management processes such as IS monitoring and incident management, for which information visualization is particularly useful, are highlighted. The visualization tasks and the requirements to visualization systems are listed. The examples of security information and event management systems (SIEM systems) that implement the requirements and solve the tasks are given. The relevance of the described solutions in light of the IS Intelligence emergence on the information protection systems' market is emphasizes.

Research Contribution

This paper highlights the main IS management processes like IS monitoring and ISIM, for which visualisation of information on IS events and incidents is needed. It formulates the visualisation tasks and requirements to visualisation systems, including a short description of SIEM systems characteristics and their impact in ISIM.

N.Miloslavskaya's contribution: Showing the role of IS monitoring and SIEM systems in solving ISIM tasks, as well as the allocation of IS information to be visualised for security decision-making (further used to define network security information to be visualised in NSICs).

Publication 03

Information Security Maintenance Issues for Big Security-Related Data

Natalia Miloslavskaya, Mikhail Senatorov, Alexander Tolstoy and Sergey Zapechnikov

Proceedings of 2014 International Conference on Future Internet of Things and Cloud FiCloud 2014. International Symposium on Big Data Research and Innovation (BigR&I). 27-29 August 2014, Barcelona, Spain.

Abstract

The need to protect big data, particularly those relating to information security (IS) maintenance (ISM) of an enterprise's IT infrastructure, is shown. A worldwide experience of addressing big data ISM issues is briefly summarized and a big data protection problem statement is formulated. An infrastructure for big data ISM is proposed. New applications areas for big data IT after addressing ISM issues are listed in conclusion.

Research Contribution

This paper emphasises the need to protect big data, particularly those relating to IS based on the analysis of a worldwide experience of ensuring IS for big data. It formulates an IS-related big data protection task and proposes the infrastructure for ensuring IS for big data.

N.Miloslavskaya's contribution: Formulation and concretisation of the IS-related big data protection task; allotment of IS-related data to be managed; the verbal description of a secure infrastructure for IS-related big data processing (further all these results were used for developing NSIC's infrastructure).

Publication 04

Information Security Theory Development

Anatoly Malyuk and Natalia Miloslavskaya

Proceedings of the 7th International Conference on Security of Information and Networks (SIN2014), September, 9-11 2014 Glasgow, UK.

Abstract

The main results obtained in formulation the informal systems theory and approaches to create simulation models of Information Security (IS) processes in conditions of incomplete and insufficient reliability of the input data, namely a unified IS concept and IS assessment methodology, are considered.

Research Contribution

This paper justifies the need for the IS theory as a new scientific direction in modern connected world of ever-growing IS incidents. It proposes an informal system theory as the scientific and methodological basis of this theory. The IS theory's content is generated based on a structured description of protection environment, comprehensive quantitative analysis of objects to be protected, system classifications of IS threats and vulnerabilities, the definition of a required object's IS level under all conditions of its operation.

N.Miloslavskaya's contribution: Joint (with the co-author) development of IS terminology for the IS theory; system classifications of IS threats and vulnerabilities.

Publication 05

Security Operations Centers for Information Security Incident Management

Natalia Miloslavskaya

Proceedings of the 4th International Conference on Future Internet of Things and Cloud (FiCloud 2016). 22-24 August 2016, Vienna Austria.

Abstract

At present information security (IS) incidents have become not only more numerous and diverse but also more damaging and disruptive. Preventive controls based on the IS risk assessment results decrease the majority but not all the IS incidents. Therefore, an IS incident management system is necessary for rapidly detecting IS incidents, minimizing loss and destruction, mitigating the vulnerabilities that were exploited and restoring the Internet of Things infrastructure (IoTI), including its IT services. These systems can be implemented on the basis of a Security Operations Center (SOC). Based on the related works a survey of the existing SOCs, their mission and main functions is given. The SOCs' classification as well as the key indicators of IS incidents in IoTI are proposed. Some serious first-generation SOCs' limitations are defined. This analysis leads to the main area of further research launched by the author.

Research Contribution

This paper is a survey of existing SOCs, their mission, and main functions. It proposes the SOCs' classification, as well as the key indicators of network attacks and their implementation as IS incidents. It describes SOC with SIEM 1.0 system for IS incident monitoring and defines some serious first-generation SOCs' limitations. This analysis leads to the main area of further research launched by the author.

Publication 06

Application of Big Data, Fast Data and Data Lake Concepts to Information Security Issues

Natalia Miloslavskaya and Alexander Tolstoy

Proceedings of 2016 4th International Conference on Future Internet of Things and Cloud Workshops. The 3rd International Symposium on Big Data Research and Innovation (BigR&I 2016). 22-24 August 2016, Vienna, Austria.

Abstract

Today we witness the appearance of some additional to Big Data concepts: data lakes and fast data. Are they simply the new marketing labels for the old Big Data IT or really new ones? Thus the key goal of the paper is to identify the relationship between these three concepts, giving special attention to their application to information security (IS) issues. The reason lies in the fact that volumes of IS-related information is one thing, but the real problem for securing enterprises' IT infrastructure assets is the speed with which things related to IS happen.

Research Contribution

This paper shows that today big data should be secured at a speed with which things related to IS happen. In the past, the "big data" term appeared. Now "data lakes" and "fast data" terms are also used. The paper tries to answer the question "Are they simply the new marketing labels for the old Big Data IT or really innovative?" Hence, the goal of the paper is to identify a relationship between these three concepts in respect to the large volumes of IS-related information.

N.Miloslavskaya's contribution: Comparison of big data, fast data and data lakes concepts and description of their relationship in respect to IS-related information.

Publication 07

Taxonomy for Unsecure Big Data Processing in Security Operations Centers

Natalia Miloslavskaya, Alexander Tolstoy and Sergey Zapechnikov

Proceedings of 2016 4th International Conference on Future Internet of Things and Cloud Workshops. The 3rd International Symposium on Big Data Research and Innovation (BigR&I 2016). 22-24 August 2016, Vienna, Austria.

Abstract

While the media constantly describes new attacks, the organizations seriously concerned about their business protection need to be prepared for such sophisticated attacks against their IT infrastructures. Hence a properly designed and formalized information security (IS) management system with Security Operations Center (SOC) as its centric part is required as never before. Among the most important documents for SOC there are two policies: IS policy and IS incident management policy. In order to create a truly effective policy it is vital to adequately describe SOC's operational environment from the IS viewpoint. The paper presents the most demand for these purposes classifications (taxonomy) of IS threats, vulnerabilities, attacks and IS incidents as the negative elements that should be avoided.

Research Contribution

This paper shows that a properly designed IS management system with a SOC as its centric part for organizations to be prepared for today's sophisticated attacks against their IT infrastructures is required as never before. For SOCs' operations, the effective IS policy and ISIM policy should be created based on a thorough description of SOCs' operational environment from the IS viewpoint. For that purpose, the paper presents a classification (taxonomy) of IS threats, vulnerabilities, attacks, and IS incidents as the negative factors, which should be excluded.

N.Miloslavskaya's contribution: Development of classification criteria for a taxonomy of IS threats, vulnerabilities, network attacks and IS incidents; examples how to use the taxonomy proposed.

Publication 08

SOC- and SIC-Based Information Security Monitoring

Natalia Miloslavskaya

A. Rocha et al. (eds.), Recent Advances in Information Systems and Technologies, Advances in Intelligent Systems and Computing. Springer International Publishing AG 2017. Vol. 570.

Abstract

New numerous and sophisticated attacks make organizations' IT infrastructure (ITI) break-in more professional and dangerously effective. The organizations must oppose this properly designed and centralized information security (IS) incident management system. Learn from the past helps to avoid the consequences of serious IS incidents in the future. Therefore, IS monitoring is necessary for rapidly detecting IS incidents, minimizing loss and destruction, mitigating the vulnerabilities exploited and restoring organization's ITI. This process can be implemented based on Security Operations Centers (SOCs) and Security Intelligence Centers (SICs) as their next evolution step. SOCs' main functions and serious limitations are defined. The SICs' concept and functioning are analyzed. The main ideas of further research conclude the paper.

Research Contribution

This paper discusses SOCs with SIEM 1.0 systems as their core for IS incident monitoring designed for rapidly detecting IS incidents, minimizing loss and destruction, mitigating the vulnerabilities exploited and restoring organizations' ITIs. After defining SOCs limitations, the paper examines the SI concept and SICs with SIEM 2.0 systems as SOCs' next evolution step for more complicated than only monitoring IS management.

Publication 09

“Network Security Intelligence” Educational and Research Center

Natalia Miloslavskaya, Alexander Tolstoy and Anton Migalin

In: Bishop M., Futcher L., Miloslavskaya N., Theocharidou M. (eds) Information Security Education for a Global Digital Society. WISE 2017. IFIP Advances in Information and Communication Technology. Springer. 2017. Vol. 503.

Abstract

The paper presents a recent experience (since 2016) in establishing and running the "Network Security Intelligence" educational and research center (NSIC) in the framework of the new NRNU MEPhI’s Institute of Cyber Intelligence Systems (ICIS). The created center is designed to provide training and research on effective network security management based on intelligent approaches and applications, the use of Big Data technologies for processing information security information, the study of the compatibility between different network protection tools, as well as the evaluation of network security. The educational NSIC’s basis currently consists of two laboratories with Next-Generation Firewall (NGFW) and Data Loss Prevention (DLP) systems at their cores respectively. Here we discuss the use of the first one. The main areas of further work in expanding NSIC’s operation for training and research conclude the paper.

Research Contribution

This paper presents a recent experience (since 2016) in establishing and running the “Network Security Intelligence” educational and research centre (NSIC) in the framework of the new MEPhI’s Institute of Cyber Intelligence Systems. The created centre is designed to provide the training of highly qualified staff for NSICs and research on effective network security management based on Security Intelligence concept and applications and big data technologies for processing IS-related information. The educational NSIC’s basis currently consists of two laboratories with Next-Generation Firewall (NGFW) and Data Loss Prevention (DLP) systems at their cores respectively. The paper discusses the use of the first one with the labs created for the training.

N.Miloslavskaya’s contribution: An idea of NSICs and their general description; description of NSIC’s implementation at the MEPhI.

Publication 10

Analysis of SIEM Systems and Their Usage in Security Operations and Security Intelligence Centers

Natalia Miloslavskaya

In: Samsonovich A., Klimov V. (eds) Biologically Inspired Cognitive Architectures (BICA) for Young Scientists. BICA 2017. Advances in Intelligent Systems and Computing, Springer, Cham. 2018. Vol 636.

Abstract

To achieve business objectives, to stay competitive and to operate legally modern organizations of all types (e.g. commercial enterprises, government agencies, not-for profit organizations), different size and sphere of activity need to match a lot of internal and external requirements. They are called compliance regulations and mean conforming to a rule, such as a specification, procedure, policy, standard, law, etc. These organizations need to ensure valuable assets, uninterrupted business operation (processes), reliable data and differentiated quality of service (QoS) to various groups of users. They need to protect their clients and employees not only inside but also outside organization itself in connection with which two new terms were introduced – teleworking or telecommuting. According to Gartner by 2020, 30 % of global enterprises will have been directly compromised by an independent group of cybercriminals or cyberactivists. And in 60 % of network breaches, hackers compromise the network within minutes, says Verizon in the 2015 Data Breach Investigations Report. An integrated system to manage organizations' intranet security is required as never before. The data collected and analyzed within this system should be evaluated online from a viewpoint of any information security (IS) incident to find its source, consider its type, weight its consequences, visualize its vector, associate all target systems, prioritize countermeasures and offer mitigation solutions with weighted impact relevance. The brief analysis of a concept and evolution of Security Information and Event Management (SIEM) systems and their usage in Security Operations Centers and Security Intelligence Centers for intranet's IS management are presented.

Research Contribution

This paper analyses two generations of SIEM systems as a core tool supporting the ISIM process. SOCs with SIEM 1.0 systems suited well for IS incident monitoring, while SIEM 2.0 systems fit well for SICs and intranets' IS management.

Publication 11

Security Intelligence Centers for Big Data Processing

Natalia Miloslavskaya

Proceedings of 2017 5th International Conference on Future Internet of Things and Cloud Workshops. The 4th International Symposium on Big Data Research and Innovation (BigR&I-2017). 21-23 August 2017, Prague, Czech Republic.

Abstract

Today numerous information security (IS) incidents in organizations' networks have become not only more sophisticated but also damaging. Hence the systems with proper security services in place to mitigate and promptly respond to IS threats by helping organizations better understand their current network situation, as well as to perform routine work in big IS-related data processing in automatic mode are needed as never before. They are known as Security Operations Centers (SOCs) and Security Intelligence Centers (SICs) as their next evolution step. The key features of SICs are summarized. The SIC business logic and data architecture are proposed. These results lead to the main area of further research.

Research Contribution

This paper analyses the evolution of IS ensuring approaches and develops the existing Security Intelligence concept for its further usage in SICs. The SIC's business logic and data architecture for big IS-related data processing are another contributions of the paper.

Publication 12

Remote Attacks Taxonomy and their Key Verbal Indicators

Natalia Miloslavskaya

Proceedings of the 8th Annual International Conference on Biologically Inspired Cognitive Architectures (BICA 2017). 1-6 August 2017, Moscow, Russia.

Abstract

To detect and to timely interrupt increasingly sophisticated attacks against modern networks, their systems, services and resources, it is especially important to understand the scenarios and phases of various possible attacks, specific for these networks. Based on the analysis of tremendous number of sources and generalizing various descriptions, remote attacks taxonomy (classification) and their key verbal indicators are proposed.

Research Contribution

This paper contributes to the understanding of various scenarios and phases of possible network attacks. Based on the analysis of many sources and standards and generalising various descriptions, it presents the remote attacks taxonomy (classification) (revised in comparison to Publication 07) and their key verbal indicators, which can be used in NSICs for composing the IoCs.

Publication 13

Information Security Management in SOCs and SICs

Natalia Miloslavskaya

Journal of Intelligent & Fussy Systems. IOS Press. Netherlands. 2018. Vol. 35, N 3.

Abstract

At present new sophisticated attacks make organizations' IT infrastructure (ITI) break-in more professional and dangerously effective. All organizations must oppose this properly designed and centralized information security (IS) management systems. Learn from the past helps to avoid the consequences of serious IS incidents in the future. Therefore, IS management is necessary for rapidly detecting IS incidents, minimizing loss and destruction caused by then, mitigating the vulnerabilities exploited and restoring organizations' ITIs. This process can be implemented based on Security Operations Centers (SOCs) and Security Intelligence Centers (SICs) as their next evolution step. SOCs' main functions and serious limitations are defined. The SICs' concept and functioning are analyzed. The main areas of further research conclude the paper.

Research Contribution

This paper is a substantially extended version of the WorldCIST2017 conference paper (Publication 08), which was proposed after its presentation at the conference to be published at the Journal of Intelligent & Fuzzy Systems. It expands in more detail the following issues: IS-related data to be managed in SOCs and SICs; SOC mission in IS monitoring; SIC mission in IS management.

Publication 14

Designing Blockchain-based SIEM 3.0 System

Natalia Miloslavskaya

Information and Computer Security. Emerald Publishing. UK. 2018. Vol. 26, Iss. 4.

Abstract

Nowadays to operate securely and legally and to achieve business objectives, secure valuable assets and support uninterrupted business processes, all organizations need to match a lot of internal and external compliance regulations such as laws, standards, guidelines, policies, specifications, procedures, etc. An integrated system able to manage information security (IS) for their intranets in the new cyberspace while processing tremendous amounts of IS-related data coming in various formats is required as never before. These data, after being collected and analyzed, should be evaluated in real-time from an IS incident viewpoint, to identify an incident's source, consider its type, weigh its consequences, visualize its vector, associate all target systems, prioritize countermeasures and offer mitigation solutions with weighted impact relevance. Different Security Information and Event Management (SIEM) systems cope with this routine and usually complicated work by rapid detection of IS incidents and further appropriate response. Modern challenges dictate the need to build these systems using advanced technologies such as the blockchain (BC) technologies. Many Internet resources argue that the BCT suits the intrusion detection objectives very well, but they do not mention how to implement it. After a brief analysis of the BC concept and the evolution of SIEM systems, the article presents the main ideas on designing the next-generation BC-based SIEM 3.0 systems, for the first time in open access publications, including a convolution method for solving the scalability issue for ever-growing BC size. This new approach makes it possible not to simply modify SIEM systems in an evolutionary manner, but to bring their next generation to a qualitatively new and higher level of IS event management in the future.

Research Contribution

This paper shows that modern IT challenges dictate the need to build SIEM systems using more advanced technologies than it was before. It lists specifications unifying the information formats applicable to IS incident description. After a brief analysis of the blockchain (BC) concept and the evolution of SIEM systems, the article presents the main ideas on designing the next-generation BC-based SIEM 3.0 systems and their architecture, including a convolution method for solving the scalability issue for ever-growing BC size. These new SIEM systems can be used as a core of NSICs because they are not simply modified SIEM systems in an evolutionary manner but bring them to a qualitatively new and higher level of IS event management.

Publication 15

Network Security Intelligence Center as a Combination of SIC and NOC

Natalia Miloslavskaya

Postproceedings of the 9th Annual International Conference on Biologically Inspired Cognitive Architectures, BICA 2018 (Ninth Annual Meeting of the BICA Society). Procedia Computer Science. 2018. Vol. 145.

Abstract

In modern networks, information security (IS) incidents have become not only numerous and diverse, but more damaging and disruptive. According to 2017 Cyber Attacks Statistics from hackmaggedon.com, among top attacks are malware, account and DNS hijacking, targeted attacks, DDoS, defacements, malvertising, and SQL injection. Various preventive controls based on IS risk assessment results decrease the majority, but not all IS incidents. Any delay and only reactive actions to IS incidents puts organization's assets under risk. Therefore, an IS incident management system has become an integral part of the whole organization's governance system. Thus, in this paper, we propose to unite together all advantages of a Security Intelligence Center and a Network Operations Center in a unified Network Security Intelligence Center (NSIC).

Research Contribution

This paper proposes to unite together all advantages of a SIC and a Network Operations Center (NOC) in a unified NSIC. It formulates the key requirements for NSICs as an integral part of the whole organization's governance system and briefly discusses its main functions in this framework.

Publication 16

Developing a Network Security Intelligence Center

Natalia Miloslavskaya

Postproceedings of the 9th Annual International Conference on Biologically Inspired Cognitive Architectures, BICA 2018 (Ninth Annual Meeting of the BICA Society). Procedia Computer Science. 2018. Vol. 145.

Abstract

In this paper, continuing our research on designing a Network Security Intelligence Center (NSIC) as a combination of a Security Intelligence Center and a Network Operations Center, we applied the PDCA approach to its development in accordance with the requirements, which we formulated for its operations and self-protection. Following the Plan stage of this approach, we proposed a five-layered NSIC's infrastructure (including platform, software, service delivery, access and management layers) and its high-level zone security infrastructure with four zones: demilitarized, trusted, restricted and management zones. All of them are briefly described in the paper. The main area of short-term further work concludes the paper.

Research Contribution

This paper is a logical continuation of Publication 15 and it proposes to apply the PDCA approach to NSIC's development in accordance with the requirements formulated for its operations and self-protection. Following the Plan stage of this approach, the paper proposes a five-layered NSIC's infrastructure (including platform, software, service delivery, access, and management layers) and its high-level zone security infrastructure with four zones: demilitarized, trusted, restricted, and management zones.

Publication 17

“Business Continuity and Information Security Maintenance" Masters' Training Program

Natalia Miloslavskaya, Mikhail Senatorov, Alexander Tolstoy and Sergey Zapechnikov

IFIP Advances in Information and Communication Technology. ISBN 978-3-642-39376-1. Ronald C. Dodge Jr., Lynn Futcher (Eds.): Information Assurance and Security Education and Training - 8th IFIP WG 11.8 World Conference on Information Security Education, WISE 8, Auckland, New Zealand, July 8-10, 2013, Proceedings, WISE 7, Lucerne Switzerland, June 9-10, 2011, and WISE 6, Bento Gonçalves, RS, Brazil, July 27-31, 2009, Revised Selected Papers. Springer. 2013. Vol. 406.

Abstract

The experience of preparing for the "Business Continuity and Information Security Maintenance" (BC&ISM) Masters’ program implementation and realization at the "Information Security of Banking Systems" Department of the National Research Nuclear University MEPhI (NRNU MEPhI, Moscow, Russia) is presented. Justification of the educational direction choice for BC&ISM professionals is given. The model of IS Master being trained on this program is described. The curriculum is presented.

Research Contribution

This paper shares the experience in designing the "Business Continuity and Information Security Maintenance" (BC&ISM) Masters’ degree programme and implementing it at the MEPhI (Moscow, Russia). It presents the model of a Master being trained in this programme and the programme’s curriculum. The results obtained can be used for the training of highly qualified staff for NSICs.

N.Miloslavskaya’s contribution: Participation in designing the programme’s content and curriculum; designing her own disciplines for the programme.

Publication 18

DLP as an Integral Part of Network Security Intelligence Center

Natalia Miloslavskaya, Victor Morozov, Alexander Tolstoy and Dennis Khassan

Proceedings of 2017 5th International Conference on Future Internet of Things and Cloud (FiCloud2017). 21-23 August 2017, Prague, Czech Republic.

Abstract

The paper presents the work-in-progress in developing since 2016 and using the "Network Security Intelligence" educational and research center (NSIC) in the framework of the NRNU MEPhI's Institute of Cyber Intelligence Systems (ICIS). The NSIC currently consists of two bearing laboratories with Next-Generation Firewall (NGFW) and Data Loss Prevention (DLP) system as their cores respectively. The DLP laboratory can be regarded as an integral NSIC's part, which expands students' knowledge and skills in protection against internal (insider) information security (IS) threats through creative research and discovery. For our NSIC the Russian SearchInform's Information Security Perimeter DLP system has been chosen. Five labs for students were developed on its basis. The main areas of further work in expanding NSIC's usage for training and research conclude the paper.

Research Contribution

This paper like Publication 09 presents the MEPhI's progress in establishing and running the NSIC and training highly qualified staff for it. The paper describes the second laboratory - DLP laboratory, which expands students' knowledge and skills in protection against internal (insider) IS threats through creative research and discovery.

N.Miloslavskaya's contribution: Further development of the NSIC concept in respect to DLP systems study in it.

Publication 19

Developing Hands-On Laboratory Works for the "Information Security Incident Management" Discipline

Natalia Miloslavskaya and Alexander Tolstoy

In: Drevin L., Theocharidou M. (eds) Information Security Education – Towards a Cybersecure Society. WISE 2018. IFIP Advances in Information and Communication Technology. Springer, Cham. 2018. Vol 531.

Abstract

The paper presents our recent experience in developing the hands-on laboratory works for the "Business Continuity and Information Security Maintenance" Master's Degree programme in the framework of the NRNU MEPhI's "Network Security Intelligence" Educational and Research Center (NSIC). These labs are designed for the "Information Security Incident Management" discipline to provide training on information security (IS) incident practical and actionable response, in particular its investigation on the basis of computer forensic approaches and specialized tools being used for these purposes. The main areas of further improvement of these labs conclude the paper.

Research Contribution

This paper presents our recent experience in developing the hands-on labs for the "Business Continuity and Information Security Maintenance" Master's degree programme, namely for the "Information Security Incident Management" discipline to provide training on IS incident actionable response, in particular, its investigation by using computer forensic approaches and specialised tools. The paper shows labs' advantages and originality: their descriptions are presented in Russian, and they take into account as much as possible the specifics of IS incidents, taking place in online banking systems.

N.Miloslavskaya's contribution: The idea of developing hands-on labs for the training of the future NSIC's staff; the content and assignments of the labs; specialised tools for the labs.

Publication 20

State-Level Views on Professional Competencies in the Field of IoT and Cloud Information Security

Natalia Miloslavskaya and Alexander Tolstoy

Proceedings of 2016 4th International Conference on Future Internet of Things and Cloud Workshops. The 3rd International Symposium on Intercloud and IoT (ICI 2016). 22-24 August 2016, Vienna, Austria.

Abstract

Two important areas of our lives – Internet of Things (IoT) and Clouds – are based on the general information and communication technologies (ICT) concepts. If so, the modern state-level requirements for the competencies of information security (IS) professionals are completely applicable to IS professionals needed for the IoT and Clouds. That is why the peculiarities of American, Australian and European approaches to the development of IS professional competencies are discussed on four best-in-the-breed examples: "The Competency and Functional Framework for IT Security Workforce Development" by the U.S. DHS/NCSD, the NICE by NIST, "The Cyber Security Capability Framework & Mapping of Information Security Manual Roles" by AGIMO and "The European e-Competence Framework" by the European Commission. Pros and cons of all approaches are marked. A short prediction on the new international standard ISO/IEC 27021 content with IS professional competencies is proposed. The discussion of all these documents' applicability to the IoT and Cloud IS professional competencies concludes the paper.

Research Contribution

This paper analyses the peculiarities of American, Australian and European approaches to the development of IS professional competencies and marks pros and cons of all approaches, as well as makes a short prediction on the international ISO/IEC 27021 standard's content. The paper proposes how to use the results obtained in the field of IoT and Clouds.

N.Miloslavskaya's contribution: Description of the peculiarities, which are applicable to the training of highly qualified staff for NSICs.

Appendix B – Confirmation Letters

To University of Plymouth

Doctoral College

Confirmation letter

With this letter I would like to confirm that my co-author Mrs. Natalia Miloslavskaya made a substantive contribution to the following publications:

1. Kostina A., Miloslavskaya N., Tolstoy A. Information Security Incident Management. Proceedings of the 3rd International Conference on Internet Technologies and Applications. 8-11 Sept 2009, Wrexham, UK. Pp. 27-34.
   N.Miloslavskaya's contribution: description of ISIM process as a whole and its subprocesses in a tabular form.

2. Miloslavskaya N., Tolstoy A., Birjukov A. Information Visualisation in Information Security Management for Enterprises's Information Infrastructure. Scientific Visualisation. Moscow, MEPhI, 2014. Vol. 6, № 2. Pp. 74-91.
   N.Miloslavskaya's contribution: showing the role of IS monitoring and SIEM systems in solving ISIM tasks, as well as the allocation of IS information to be visualised for security decision-making.

3. Miloslavskaya N., Senatorov M., Tolstoy A, Zapechnikov S. Information Security Maintenance Issues for Big Security-Related Data. Proceedings of 2014 International Conference on Future Internet of Things and Cloud FiCloud 2014. International Symposium on Big Data Research and Innovation (BigR&I). 27-29 August 2014, Barcelona (Spain). Pp. 361-366. DOI: 10.1109/ FiCloud.2014.64.
   N.Miloslavskaya's contribution: formulation and concretisation of the IS-related big data protection task; allotment of IS-related data to be managed; the verbal description of a secure infrastructure for IS-related big data processing (further all these results were used for developing NSIC's infrastructure).

4. Miloslavskaya N., Tolstoy A. Application of Big Data, Fast Data and Data Lake Concepts to Information Security Issues. Proceedings of 2016 4th International Conference on Future Internet of Things and Cloud Workshops. The 3rd International Symposium on Big Data Research and Innovation (BigR&I 2016). 22-24 August 2016, Vienna (Austria). Pp. 148-153. DOI: 10.1109/W-FiCloud.2016.41.
   N.Miloslavskaya's contribution: comparison of big data, fast data and data lakes concepts and description of their relationship in respect to IS-related information.

5. Miloslavskaya N., Tolstoy A., Zapechnikov S. Taxonomy for Unsecure Big Data Processing in Security Operations Centers. Proceedings of 2016 4th International Conference on Future Internet of Things and Cloud Workshops. The 3rd International Symposium on Big Data Research and Innovation (BigR&I 2016). 22-24 August 2016, Vienna (Austria). Pp. 154-159. DOI: 10.1109/W-FiCloud.2016.42.
   N.Miloslavskaya's contribution: development of classification criteria for a taxonomy of IS threats, vulnerabilities, network attacks and IS incidents; examples how to use the taxonomy proposed.

6. Miloslavskaya N., Tolstoy A., Migalin A. "Network Security Intelligence" Educational and Research Center. In: Bishop M., Futcher L., Miloslavskaya N., Theocharidou M. (eds) Information Security Education for a Global Digital Society. WISE 2017. IFIP Advances in Information and Communication Technology. Springer. 2017. Vol. 503. Pp. 157-168. DOI: 10.1007/978-3-319-58553-6_14.
N.Miloslavskaya's contribution: an idea of NSICs and their general description; description of NSIC's implementation at the MEPhI.

7. Miloslavskaya N., Senatorov M., Tolstoy A., Zapechnikov S. "Business Continuity and Information Security Maintenance" Masters' Training Program. IFIP Advances in Information and Communication Technology. Ronald C. Dodge Jr., Lynn Futcher (Eds.): Information Assurance and Security Education and Training - 8th IFIP WG 11.8 World Conference on Information Security Education, WISE 8, Auckland, New Sealand, July 8-10, 2013, Proceedings, WISE 7, Lucerne Switzerland, June 9-10, 2011, and WISE 6, Bento Gonçalves, RS, Brasil, July 27-31, 2009, Revised Selected Papers. Springer 2013. Vol. 406. Pp. 95-102. DOI: 10.1007/978-3-642-39377-8_10.
N.Miloslavskaya's contribution: participation in designing the programme's content and curriculum; designing her own disciplines for the programme.

8. Miloslavskaya N., Morozov V., Tolstoy A., Khassan D. DLP as an Integral Part of Network Security Intelligence Center. Proceedings of 2017 5th International Conference on Future Internet of Things and Cloud (FiCloud2017). 21-23 August 2017, Prague (Czech Republic). Pp. 297-304. DOI 10.1109/FiCloud.2017.15.
N.Miloslavskaya's contribution: further development of the NSIC concept in respect to DLP systems study in it.

9. Miloslavskaya N., Tolstoy A. Developing Hands-On Laboratory Works for the "Information Security Incident Management" Discipline. 2018. In: Drevin L., Theocharidou M. (eds) Information Security Education – Towards a Cybersecure Society. WISE 2018. IFIP Advances in Information and Communication Technology. Springer, Cham. 2018. Vol 531. Pp. 28-39. DOI: 10.1007/978-3-319-99734-6_3.
N.Miloslavskaya's contribution: the idea of developing hands-on labs for the training of the future NSIC's staff; the content and assignments of the labs; specialised tools for the labs.

10. Miloslavskaya N., Tolstoy A. State-Level Views on Professional Competencies in the Field of IoT and Cloud Information Security. 2016. Proceedings of 2016 4th International Conference on Future Internet of Things and Cloud Workshops. The 3rd International Symposium on Intercloud and IoT (ICI 2016). 22-24 August 2016, Vienna (Austria). Pp. 83-90. DOI: 10.1109/W-FiCloud.2016.31.
N.Miloslavskaya's contribution: description of the peculiarities, which are applicable to the training of highly qualified staff for NSICs.

Associate Professor Alexander Tolstoy

Moscow, 25 December 2018

To University of Plymouth

Doctoral College

Confirmation letter

This letter confirms that my co-author Associate Professor Natalia Miloslavskaya made a substantive contribution to the following publications:

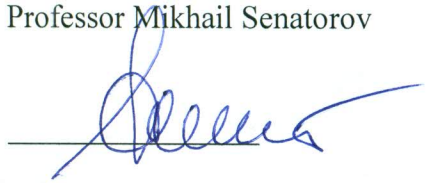
1. Miloslavskaya N., Senatorov M., Tolstoy A, Zapechnikov S. Information Security Maintenance Issues for Big Security-Related Data. Proceedings of 2014 International Conference on Future Internet of Things and Cloud FiCloud 2014. International Symposium on Big Data Research and Innovation (BigR&I). 27-29 August 2014, Barcelona (Spain). Pp. 361-366. DOI: 10.1109/ FiCloud.2014.64.

   Miloslavskaya's contribution: Formulation and concretisation of the IS-related big data protection task; allotment of IS-related data to be managed; the verbal description of a secure infrastructure for IS-related big data processing.

2. Miloslavskaya N., Senatorov M., Tolstoy A., Zapechnikov S. "Business Continuity and Information Security Maintenance" Masters' Training Program. IFIP Advances in Information and Communication Technology. Ronald C. Dodge Jr., Lynn Futcher (Eds.): Information Assurance and Security Education and Training - 8th IFIP WG 11.8 World Conference on Information Security Education, WISE 8, Auckland, New Sealand, July 8-10, 2013, Proceedings, WISE 7, Lucerne Switzerland, June 9-10, 2011, and WISE 6, Bento Gonçalves, RS, Brasil, July 27-31, 2009, Revised Selected Papers. Springer 2013. Vol. 406. Pp. 95-102. DOI: 10.1007/978-3-642-39377-8_10.

   Miloslavskaya's contribution: Participation in designing the programme's content and curriculum; designing her own disciplines for the programme.

Professor Mikhail Senatorov



Moscow, December 21, 2018

To University of Plymouth

Doctoral College

Confirmation letter

With this I would like to confirm that my co-author Mrs. Natalia Miloslavskaya made a substantive contribution, namely the joint development of terminology for the IS theory and system classifications of IS threats and vulnerabilities, to the original work

Malyuk A., Miloslavskaya N. Information Security Theory Development. Proceedings of the 7th International Conference on Security of Information and Networks (SIN2014), 9-11 September 2014. Glasgow (UK). ACM New York. Pp. 52-55. DOI: 10.1145/2659651.2659659.

Professor Anatoly Malyuk

December 24, 2018, Moscow

To University of Plymouth

Doctoral College

Confirmation letter

I would like to confirm that my co-author Dr. Natalia Miloslavskaya made a substantive contribution to the works listed below:

1) Miloslavskaya N., Senatorov M., Tolstoy A, Zapechnikov S. Information Security Maintenance Issues for Big Security-Related Data. Proceedings of 2014 International Conference on Future Internet of Things and Cloud FiCloud 2014. International Symposium on Big Data Research and Innovation (BigR&I). 27-29 August 2014, Barcelona (Spain). Pp. 361-366. DOI: 10.1109/ FiCloud.2014.64.

Dr. Miloslavskaya's contribution: formulation and concretisation of the IS-related big data protection task; allotment of IS-related data to be managed; the verbal description of a secure infrastructure for IS-related big data processing.

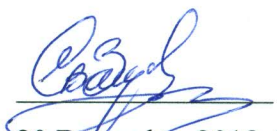
2) Miloslavskaya N., Tolstoy A., Zapechnikov S. Taxonomy for Unsecure Big Data Processing in Security Operations Centers. Proceedings of 2016 4th International Conference on Future Internet of Things and Cloud Workshops. The 3rd International Symposium on Big Data Research and Innovation (BigR&I 2016). 22-24 August 2016, Vienna (Austria). Pp. 154-159. DOI: 10.1109/W-FiCloud.2016.42.

Dr. Miloslavskaya's contribution: development of classification criteria for a taxonomy of IS threats, vulnerabilities, network attacks and IS incidents; examples how to use the taxonomy proposed.

3) Miloslavskaya N., Senatorov M., Tolstoy A., Zapechnikov S. "Business Continuity and Information Security Maintenance" Masters' Training Program. IFIP Advances in Information and Communication Technology. Ronald C. Dodge Jr., Lynn Futcher (Eds.): Information Assurance and Security Education and Training - 8th IFIP WG 11.8 World Conference on Information Security Education, WISE 8, Auckland, New Sealand, July 8-10, 2013, Proceedings, WISE 7, Lucerne Switzerland, June 9-10, 2011, and WISE 6, Bento Gonçalves, RS, Brasil, July 27-31, 2009, Revised Selected Papers. Springer 2013. Vol. 406. Pp. 95-102. DOI: 10.1007/978-3-642-39377-8_10.

Dr. Miloslavskaya's contribution: participation in designing the programme's content and curriculum; designing her own disciplines for the programme.

Professor Sergey Zapechnikov



20 December 2018, Moscow

To University of Plymouth

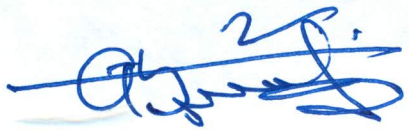
Doctoral College

Confirmation letter

With this confirmation letter I would like to state that my co-author Associate Professor N.Miloslavskaya made a substantive contribution to the work

Miloslavskaya N., Tolstoy A., Birjukov A. Information Visualisation in Information Security Management for Enterprises's Information Infrastructure. Scientific Visualisation. Moscow, MEPhI, 2014. Vol. 6, № 2. Pp. 74-91.

In this publication, she emphasizes the role of IS monitoring in Information Security Management for Enterprises's Information Infrastructures and shows the role of SIEM systems in solving IS incident management tasks. Besides this, she defines IS information to be visualised for security decision-making.

Associate Professor Alexander Birjukov 

Moscow

December 25, 2018

To University of Plymouth

Doctoral College

Confirmation letter

With this letter I would like to confirm that my co-author Natalia Miloslavskaya made a substantive contribution to the publication

Miloslavskaya N., Morozov V., Tolstoy A., Khassan D. DLP as an Integral Part of Network Security Intelligence Center. Proceedings of 2017 5th International Conference on Future Internet of Things and Cloud (FiCloud2017). 21-23 August 2017, Prague (Czech Republic). Pp. 297-304. DOI 10.1109/FiCloud.2017.15.

Development and description of the NSIC's concept in respect to DLP systems usage and study in it is her essential contrtibution to this work.

Associate Professor Victor Morozov

Moscow, 26th of December, 2018.

To University of Plymouth

Doctoral College

Confirmation letter

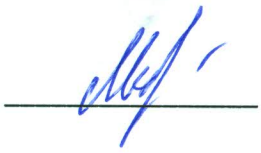
Hereby I would like to confirm that my co-author Associate Professor N.Miloslavskaya made a substantive contribution to the work

Miloslavskaya N., Tolstoy A., Migalin A. "Network Security Intelligence" Educational and Research Center. In: Bishop M., Futcher L., Miloslavskaya N., Theocharidou M. (eds) Information Security Education for a Global Digital Society. WISE 2017. IFIP Advances in Information and Communication Technology. Springer. 2017. Vol. 503. Pp. 157-168. DOI: 10.1007/978-3-319-58553-6_14,

as the idea of NSICs belongs to her.

In this publication, she gives a general description of a NSIC and its implementation at the MEPhI, at the "Information Security of Banking Systems" Department.

Anton Migalin



Moscow, 20 December 2018

To University of Plymouth

Doctoral College

Confirmation letter

Hereby I would like to confirm that my co-author Mrs. Natalia Miloslavskaya made a substantive contribution to the original work

Kostina A., Miloslavskaya N., Tolstoy A. Information Security Incident Management. Proceedings of the 3rd International Conference on Internet Technologies and Applications. 8-11 Sept 2009, Wrexham, UK. Pp. 27-34,

in particular in the description of IS incident management process as a whole and its subprocesses in a tabular form.

Anna Kostina

December 19, 2018

Moscow

To University of Plymouth

Doctoral College

Confirmation letter

I confirm that my co-author Associate Professor Natalia Miloslavskaya made a substantive contribution to the work

Miloslavskaya N., Morozov V., Tolstoy A., Khassan D. DLP as an Integral Part of Network Security Intelligence Center. Proceedings of 2017 5th International Conference on Future Internet of Things and Cloud (FiCloud2017). 21-23 August 2017, Prague (Czech Republic). Pp. 297-304. DOI 10.1109/FiCloud.2017.15

while developing her own NSIC's concept in respect to DLP systems usage and study within the framework of this NSIC allocated in the MEPhI.

Dennis Khassan

December 27, 2018

Moscow