Security Operations Centers for Information Security Incident Management

Natalia Miloslavskaya
National Research Nuclear University MEPhI (Moscow Engineering Physics Institute)
Moscow, Russia
NGMiloslavskaya@mephi.ru

***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.**

Keywords—information security, information security incidents, Internet of Things, information security monitoring, Security Operations Center

I. INTRODUCTION

In modern conditions a lot of work has been done in the direction of an organization's IS maintenance, but little proposed for the management of IS controls implemented for the fast-moving field of the Internet of Things (IoT). The IoT is a global infrastructure, enabling advanced services by interconnecting physical and virtual things based on the information and communication technologies existing and evolving interoperable [1]. In a simplest view the IoT is the network of physical objects that enables them to collect and exchange data. Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled. We often do not realize what assets of the IoT infrastructure (IoTI) are more critical, what IS risks are associated with these assets, what IS controls should be planned for them and why. These and many other questions can be answered as a result of different IS checks, including the IS monitoring and control of the security measures used (collectively called IS monitoring).

IS monitoring is understood as a permanent (continuous) elicitation of events to be registered as affecting IS maintenance in a particular environment (IT, system, network, service and IoTI), as well as the collection, analysis and generalization 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 normal mode of the environment functioning) [2]. The common and more specialized information protection tools (IPTs) can register millions of IS events of different origins and consequences in the intranets of large organization as well as in the emerging IoTI during one day only. 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. Unfortunately, this activity, often manual and time-consuming, can overwhelm the most experienced professionals. Timely and constant data observation, collection, analysis and processing for each of the IS maintenance activities in accordance with the intended purposes, as well as provision of the authorized parties with full, timely, reliable information for justified decision-making in the sphere of IS maintenance are the main objectives of the IS monitoring.

Analyzing IS monitoring data usually pursues the following purposes:

- Control over implementation of the provisions of internal and external IS maintenance documents in order to detect deviations from the accepted business and IS maintenance requirements (e.g., fixed in the logical access to IoTI assets policy);
- Quality control (by which the efficiency and effectiveness are meant) of the security measures used;
- Recognition of the contingencies, including malicious, with IoTI assets and business processes;
- Detection of IS events, partly further classified as IS incidents;
- Detection of the IoTI assets' vulnerabilities that attackers can use to implement attacks on the systems, networks and services, its business partners and users of public networks such as the Internet alike;
- Providing evidence in case of computer crimes investigation.

IS events and incidents detection, reporting and response are the core of IS monitoring operations. According to the special international standard ISO/IEC 27035:2011 «Information technology -- Security techniques -- Information security incident management» it is essential for any organization serious about IS to have an effective IS Incidents

978-1-5090-4052-0/16 $31.00 © 2016 IEEE
DOI 10.1109/FiCloud.2016.26

IEEE computer society

Authorized licensed use limited to: ISRO Telemetry Tracking and Command Network. Downloaded on February 06,2025 at 09:03:07 UTC from IEEE Xplore. Restrictions apply.

Management Process (ISIMP). ISIMP is a basic part of the general IS management processes and a structured and planned approach to [3]:

- Detect, report and assess IS events and IS incidents;
- Respond to IS incidents, including the activation of appropriate controls for the prevention and reduction of, and recovery from, impacts;
- Report vulnerabilities that have not yet been exploited to cause IS events and possibly IS incidents, and assess and deal with them appropriately;
- Learn from IS incidents, institute preventive controls, and, over time, make improvements to the overall IS incident management.

The constant stream of various data about IoTI's well-being from many devices, log managers, SIEM systems and other IoTI's network security management interfaces creates quite a load on IS staff. In the noise of all events and IS-related data, it is difficult to sort through and obtain real, actionable IS events that need attention and immediate response. The dramatically increased by that time complexity of IS monitoring faced by the network security administrators urgently demanded new universal high performance solutions that bring reporting, analysis, modelling, planning and collaboration together for better visibility and decision-making. So a specialized Security Operations Center (SOC) with the right IPTs and skilled staff in place as a heart of a good IS incident management process has been appeared in the late 1990's.

Thus, the remainder of the paper is organized as follows. In section 2 the related works in the area are briefly analyzed. The interrelation of ISIMP and IS monitoring is shown in section 3. Section 4 describes the SOCs' mission in IS incident management. The SOCs classification is given in Section 5. The key verbal indicators of IS incidents in IoTI are proposed in Section 6. Some serious first-generation SOCs' limitations are defined in Section 7. The indication of main area of further research concludes the paper.

II. Related works

Now there are a sufficient number of international documents that regulate various aspects of IS incident management (ISIM). As a rule, all these documents consistently consider all ISIMP stages: from process planning to its improvement after the analysis of the results of the process itself.

ISO/IEC 27001 «Information technology -- Security techniques -- Information security management systems -- Requirements» [4] contains the requirements for organization's IS management system (ISMS) development regardless of its activities and imposes some of the general requirements for IS management processes, including ISIMP as its integral part, for example:

- ISMS establishing, implementing, maintaining and continually improving;
- Proper documentation of processes and procedures;
- Management commitment to all IS management processes.

According to the 9.1 «Monitoring, measurement, analysis and evaluation» clause of [5] the following requirements should be executed during ISIMP:

- Detect errors in the results of processing;
- Identify attempted and successful IS breaches and incidents;
- Help to detect IS events and thereby prevent IS incidents by the use of indicators;
- Determine whether the actions taken to resolve an IS breach were effective;
- Enable management to determine whether the security activities delegated to people or implemented by IT and IPTs are performing as expected.

NIST Special Publication 800-61 «Computer security incident handling guide» represents the collection of the best practices in the field of processes construction for response to computer security incidents [5]. However IS incident is wider than computer security incidents. The group of software and technical incidents, including computer security incidents, is only one of its components.

The computer security incident handling process is examined in detail from initial planning to an incident analysis after the ending of response process, namely:

- Creating an IS incident response policy and plan;
- Developing procedures for performing IS incident handling and reporting;
- Setting guidelines for communicating with outside parties regarding IS incidents;
- Selecting a team structure and staffing model;
- Establishing relationships and lines of communication between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies);
- Determining what services the incident response team should provide;
- Staffing and training the incident response team.

A number of works [6-8] describes the technique and gives a framework for planning, implementation, assessment and improvement of ISIMP. The main attention is given to the organization of an IS incidents response teamwork. The order of interaction of various participants' roles during incident management processes is determined. The use of a role principle allows allocating employees with additional duties within the scope of ISIMP without a binding to their posts and official duties. It is stressed out that ISIMP can be implemented in different ways depending on conditions in which it will operate.

The majority of works deserving special attention on SOCs have been published in the late 1990's and early 2000's [9-19]. Cisco Systems Inc. contribution to the SOC idea, its building, operating and maintaining should be mentioned especially as it cannot be overestimated since 1998 till nowadays [20]. Subsequent publications are more focused in scope and cover mostly tools for computer network defense [21-24]. They focus either on technology (while excluding people and process) or

Authorized licensed use limited to: ISRO Telemetry Tracking and Command Network. Downloaded on February 06,2025 at 09:03:07 UTC from IEEE Xplore. Restrictions apply.

cover people and process at length without bringing in the elements of technology and tools.

III. Interrelation of IS Incident Management Process and IS Monitoring

ISO/IEC 27043:2015 «Information technology -- Security techniques -- Incident investigation principles and processes» [25] describes typical activities surrounding IS incident and its investigation (Figure 1). After detecting an IS event (e.g. reconnaissance, unsuccessful or non-compliance user's activity attempt, explained anomaly, etc.) the organization's Operation Assurance Group conducts its first assessment. If it shows that this event is an IS incident (such as DoS attack, root or user level intrusion, virus infection, malicious logic, etc.), the IS Incident Response Team (ISIRT) conducts a second, more detailed assessment. It is also detected, whether the IS incident is under control. If not and the consequences of the IS incident are serious, anti-crisis measures may be required.

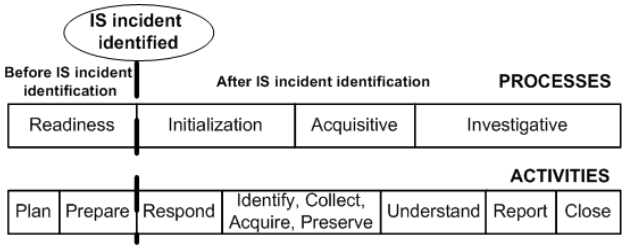

Fig. 1. Typical activities for IS incident handling

IS monitoring is closely associated with the IS incident management. Preparing to collect the necessary data, data collection itself, filtering and analysis of the collected data, data management, DB management of the collected information, etc. are the IS monitoring processes associated with the IS incident management (Figure 2) [2].

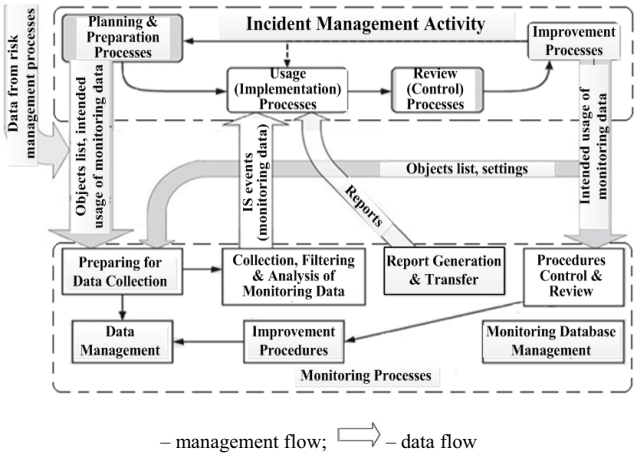

Fig. 2. IS monitoring and IS incident management processes interrelation

IS monitoring data is used directly for the IS incident management, 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.

Effective IS incident management provides rapid restoration of normal IoTI's functioning, minimizes their adverse impact on the business and, most importantly, prevents their possible occurrence in the future by selecting and implementing adequate controls to the problems identified (IS threats and vulnerabilities).

The data accumulated within ISIMP are necessary for many other ISMS's processes, for example, for carrying out a correct IS risk assessment including existing security measures and IS management processes. Ultimately, in relationship with other IS management processes, ISIMP can help to assess the overall IoTI IS level. A sufficient IS level within IoTI should be provided and maintained for a long time to counter IS threats, to reduce IS risks and to efficient IS events and incidents processing. All these benefits become even more valuable for distributed IoTI with actively used networks. All this determines the presence of a large number of applicable IS threats that could become real IS incidents.

IV. Security Operations Centers Mission in IS Incident Management

We face today many challenges in heterogeneous and highly distributed IoTI. Handling an increasing IoTI complexity with the existing head-count are challenges that will continue into the foreseeable future. Two important sources of complexity are the vast quantity and variety of security alarms detected and reported by identity access management (IAM) systems, anti-viruses (AVs), intrusion detection and prevention systems (IDPSs), firewalls (FWs), Unified Threat Management (UTM) systems, OSs, security appliances (SAPP), security information and event management (SIEM) systems, etc. and the diversity of tasks performed by IS department including management of assets, risks, IPTs, patching, IS incidents and IS-related information, encryption, etc.

A single FW alone can produce over gigabytes of log data daily and an IDPS can produce over millions messages over the same period. A part of the information generated by the IPTs is dominated by false positives (an indication of hostile activity when there is none). Most of the messages are simply artifacts of normal and legitimate use of IoTI's resources. The problem is to isolate and prioritize the few messages that do indeed indicate the real IS threats and events. The need to isolate significant IS incidents from the white noise of IAM, AV, IDPS, FW, UTM, OS, SAPP and SIEM messages is critical and it is a part of the larger economic reality requiring to utilize the existing security measures more effectively.

The key to a more effective automation of security operations workload and prioritization of the ISM tasks including rapid response to known or emerging IS threats lies in setting up its in-house specialized unit before IoTI may be compromised. This unit is known as a Security Operations Center (SOC) which we defined as is a centralized unit that

Authorized licensed use limited to: ISRO Telemetry Tracking and Command Network. Downloaded on February 06,2025 at 09:03:07 UTC from IEEE Xplore. Restrictions apply.

deals with security issues on an organizational level plus a team primarily composed of security analysts organized to detect, analyze, respond to, report on, and prevent IS incidents [26]. SOC manages all security operations and in particular monitors, assesses and protects its information and other sensitive areas like DBs, servers, networks, websites, etc.

From our point of view SOC is a nucleus of network security operations (as a main IoTI's part), providing continuous protection, detection and response capabilities against IS threats, remotely exploitable constant and continuous protection vulnerabilities and real-time IS incidents on the network. With a first-generation SIEM system as a core component, SOC as a shared ISM service center centrally collects data from tens and hundreds of IPTs (IAM, AVs, IDPSs, FWs, etc.) and combines all the fundamental components of an excellent security system into a productive, real-time analysis center, building an overall IS picture for IoTI and helping to quickly sort out setting. Its output gives a logical picture of the security health of the network and instant response to critical issues and vulnerabilities. SOC integrates security and network event information, giving security and operations staff necessary data to make informed decisions within a zero-day response window.

Any SOC eliminates the need to manually research, gather, evaluate, categorize, analyze and ultimately identify IS incidents-related information from multiple sources across the intranet, extranet and even the internet [20]. Its main goal can be formulated as to effectively incorporate human and dynamic computer more informed decision-making in the field on network security in order to minimize its IS risks.

At the implementation of such a hybrid approach, individual automated correlations and their interpretations can be connected into a large single or few smaller separate workflows, supported by both manual and automated approval steps. Thus at first SOC should have possibility and all necessary software and hardware tools in place to respond to advanced IS threats, to analyze its internal, external and perimeter network connections, to detect on time the early stages of DDoS attack and to thwart it, to assist in digital forensics of IS breaches and much more. Not every IS breach necessarily means that the business will immediately experience critical negative impact, as attackers usually need time to fulfill a few preliminary steps beyond gaining unauthorized access to a separate network element or entire network. Accurately discovering and timely preventing this type of behavior is just one of the many tasks that must be solved by a SOC. In these conditions areas for consideration include network analysis, media and devices monitoring, anomaly and misuse detection, malware protection, event correlation and security information and event management systems, etc.

In the second place any SOC should have a few operators entering data and security analysts on staff that focuses solely on analytics (their number certainly depends on IoTI's size and complexity) [20]. They perform in-depth and consolidated analysis of unknown and not previously encountered IS events, just emerging IS threats, new attacks characteristics (such as APTs), zero-day vulnerabilities. They have a firm grasp on local, regional and global environment and events that could affect IoTI operations and assets.

In IoTI SOC works in a round-the-clock mode (consistent operation) and performs the following typical functions:

- SOC's Operational Support System with a Command Console being used to execute various commands for advanced administrating, troubleshooting and solving certain kinds of issues;
- IoTI Asset Tracking and Recovery aimed at supporting allocation of IoTI resources in order to successfully recover damages caused by different IS incidents;
- Vulnerability Scanning followed by Patch Management as a special security function allowing to proactively reveal IoTI resources' vulnerabilities before an attacker will identify them and gain any benefit conceived and subsequent installing appropriate security patches to these administered resources;
- Traffic Sniffing for capturing any data passed in packets over the network channels and looking for any information that may be useful for troubleshooting and IS incident detection at least;
- Device Configuration Management designed for automation and taking total control of the entire life cycle of all IoTI components (such as switches, routers, FWs and other network devices' configurations);
- Centralized Management of IPTs (such as IAM/AV/FW/IDPS, etc.) implementing the idea to centrally manage the process of their configuring, deploying security policies, evaluating their status, generating reports on their operation across your entire IoTI and so on;
- IS Risk Management and Risk Ranking based on Business Impact Analysis, including passive IS risk assessment and active IS risk treatment, monitoring, communication, etc. The process input is any information collected during SOC's functioning and from another consolidated and trusted information sources selected;
- Security Information Management for log collection, storage, archiving and historical reporting;
- IS Events and Incidents Handling, consisting of Detection, Alerting and Notification, Reporting and Response [3] as the core of security operations with continuous cyclic feedback mechanism driving incident handling and Escalation Management (know who to communicate during an IS incident);
- A local in-house ISIRT (IS incident response team) that collaborates with National Computer emergency response team (CERT);
- Data and Computer Forensics allotted for reconstructing series of events during an IS incident and examining digital media (including computer equipment) in a forensically sound manner to identify, gather, preserve, recover, analyze and present facts and digital evidence related to various IS incidents and computer crime eventually.

For example, SOC could help in identifying actors who may be targeting its employees, such as phishing attacks conducted via email or more globally to reduce vulnerabilities and any related IS risk and primarily focus on the business.

Authorized licensed use limited to: ISRO Telemetry Tracking and Command Network. Downloaded on February 06,2025 at 09:03:07 UTC from IEEE Xplore. Restrictions apply.

Detection of the well-known botnet server's IP address inside IoTI's network likely indicates that one or more of its systems have been compromised. Another typical unwanted and suspicious event is a DB or files access from one of IoTI's devices via a USB memory device. This event can indicate that one of the IS policies, namely a policy restricting USB usage, has been violated and that a security control supporting it has been circumvented.

For its operation SOC uses different extracting, filtering, normalization, categorization, correlation and the other analysis techniques and heuristics to determine which malicious IP addresses, URLs, applications or something else could harm IoTI's resources and to understand which IoTI assets' vulnerabilities are most often exploited by attackers.

The SOC's effectiveness is reasonable measured by how IS incidents are managed, handled, administered, remediated and isolated.

V. SOCs Types

There are many well-known solutions offering this kind of functionality, which differ by cost, performance and implemented features. Current SOCs can be described from different points of view (Table 1). Their main characteristics are counteraction capabilities, deployment scenarios, aim, correlation technique (correlation is considered as dependency between entities within SOC), implementation variant and ownership. The given classification does not pretend to completeness and may be broadened if necessary.

TABLE 1. SOC CLASSIFICATION (TO BE CONTINUED)

Classification parameters	*Parameter content*	*Description*
1. Counteraction capabilities	1.1 SOC without such a capability	SOC acts like classical IDS: it monitors and prioritizes IS events. In case an attack is detected, no response actions are executed. SOC is usually used in the environments with high demands for availability (for example, in banking or medicine) because false positives do not lead to new security rules creation and services blocking. Main SOC's objectives: IS data processing, IS events visualization and prioritization and regulatory compliance. (E.g., Netforensics Open System Platform Software, CA eTrust Security Information Management Solution.)
	1.2 Reactionary SOC	SOC utilizes IPS concept: the attack is not only detected, but also mitigation functions are performed to stop the attack propagation. SOC understands all attack's components, down to the offending and compromised system addresses. Auto mitigation identifies available «choke-point» devices along the attack path and automatically provide the appropriate device commands that can be employed to mitigate the risk. The results can be used to quickly and accurately prevent or contain the attack. SOC is commonly used within the environments with high demands for confidentiality. Quick automatic response to IS threats is its key advantage. (E.g., Cisco Monitoring Analysis and Response System, IBM Tivoli Security Operation Manager Software, Check Point Eventia Analyzer.)
2. Deployment scenarios	2.1 centralized	SOC is based on a dedicated device/server which performs all functions related to IS management. The advantages: speed, ease of installation and relatively low cost. The drawback: SOC is appropriate only to small-to-medium environments (<100 IPTs).
	2.2 distributed	SOC utilizes several devices/servers simultaneously performing load balancing between them. Load distribution can be based either on geographical principle (different servers are responsible for different parts of the network) or on functional principle (part of the functions is performed by one server, part by another). Because multiple devices are used, SOC's cost is greater and the deployment and maintenance is more complex. Though load balancing results in better performance and effective SOC overall.
3. SOC aim	3.1 controlling	SOC allows to observe the protected objects' IS level and to forecast its change.
	3.2 managed	SOC helps to actively operate objects' IS.
	3.3 crisis	SOC begins to act only during the crisis.
4. Correlation technique	4.1 statistical	SOC applies statistical algorithms to determine IS incident severity and then assigns an IS threat score based on asset value. It looks at network behavior and identifies IS threats based on the presence and likely severity of anomalous event patterns. It also allows to measure effectiveness, as the number of anomalous events should decrease over time as IoTI becomes more secure. The advantages: does not require specific knowledge of IS threat patterns or attack scenarios to work and is an operational technology that does not require the definition of rules or significant «baselining» (determining a statistically normal state) prior to implementation. This means the near-term help in prioritizing IS events based on IoTI asset value.
	4.2 rule-based	SOC uses predefined rules that apply conditional logic to identify likely attack scenarios by observing a specific series of events within a specified time slot. Rules can be delivered «out of the box» by a SOC vendor, or implemented on a custom basis after careful analysis of network traffic. This correlation is extremely effective at identifying specific IS threats based on prior knowledge of attack patterns. Many products implement a finite set of rules that cover common scenarios, and these can be extended with custom rules. The correlation effective depends on the SOC vendor's support for maintaining rule state. A rule must be a long-running event, and the rules engine must hold events «in state» for a reasonable period of time until other qualifying events either trigger an alert or the rule times out for the initial event. Without this, we will experience numerous false positives, or more importantly, fail to identify «low and slow attacks» which are characterized by a small number of daily events over a long time slot. Among the drawbacks are time consuming of keeping up-to-date hundreds of rules, too many false positives and false negatives for constantly innovative attackers techniques.

Authorized licensed use limited to: ISRO Telemetry Tracking and Command Network. Downloaded on February 06,2025 at 09:03:07 UTC from IEEE Xplore. Restrictions apply.

TABLE 1. SOC CLASSIFICATION (THE END)

Classification parameters	*Parameter content*	*Description*
4. Correlation technique	4.3 vulnerability	SOC takes IS event data from network IDSs and correlates it against a DB of known vulnerabilities, and host vulnerability profiles returned by vulnerability management scanners, returning a score for each asset. It helps eliminate false positives by reducing «scanner noise», and helps security personnel determine which attacks are real, and which assets are actually vulnerable to the attack. The advantages: the most effective at spotting specific attack scenarios, including those scenarios that might be new to IoTI, and extremely good at eliminating false positives and maximizing the efficiency by focusing on real IS events that correspond to true vulnerabilities. The drawbacks: if it requires rule creation to correlate attacks that exploit particular vulnerabilities with susceptible assets, because writing these rules would be extremely labor-intensive.
	4.4 Service Level Agreement (SLA)	SIC binds IS events to SLA requirements and is very important for business because it helps to evaluate losses from compromised network elements or components rendered out of service. SOC builds business-processes models and analyses impact on these processes from different IS incidents. The drawback: main difficulties are business-processes composition and assets cost determination (the difficulties which are natural for process-oriented risk analysis in IT).
	4.5 compliance	SOC binds IS events to existing laws, IS policies and standards (both corporate and regulatory). It needs special setup and configuration because only static binding is possible since every IoTI has its own IS policy.
	4.6 mixed	When all types of correlation are applied together, they can greatly improve the detection of real attacks and the effectiveness of IS management. When security staff can get a unified risk profile of events based on a statistical threat score, rule-based alerts triggered, associated vulnerabilities, and asset value, their job is much easier.
	4.7 SOC without correlation	SOC is appropriate for small networks where SOC performs only IS data aggregation and all the decisions are performed by the security team.
5. Implementation variant	5.1 software	SOC is built upon specialized software installed on one/ several servers. The advantage: the possibility to use SOC servers for additional tasks.
	5.2 hardware	SOC is out-of-the-box solution which is based on one/several servers with pre-installed SOC software. The advantage: decreased deployment time. Since it has isolated environment, no additional software can be installed on SOC servers.
	5.3 infrastructure solution	SOC is built using existing software and hardware (E.g., existing Oracle DB is used for IS event storage. Security DBs consolidation is implemented using Oracle replication techniques. Normalization, aggregation and correlation capabilities are implemented within the DB using SQL scripts, etc.). The advantages: relatively low cost of the solution and increased flexibility. The drawbacks: the need to develop SOC including normalization, aggregation and correlation rules and SQL-programming to implement these rules.
6. Ownership	6.1 in-hose	Advantages: knowledge about IoTI is higher than by third-party, more effective, solutions are easier to customize, most likely to notice correlations within IoTI, better tool pricing. Drawbacks: large up-front investments, need to show effectiveness quickly, high potential for «intruder-monitoring team» collusion, less likely to recognize large-scale patterns accumulated by long-time experience of specialized third-parties.
	6.2 outsourced	Advantages: no capital expenses, often cheaper, less potential for «intruder-monitoring team» collusion, unbiased, SLA. Drawbacks: less knowledge about IoTI; decrease in staff vigilance, risk of external data mishandling; no long-term gain for IoTI.

VI. KEY INDICATORS OF IS INCIDENT

The main sources of IS events in SOCs are technical, software and hardware tools of IS monitoring and operation control of the security measures used.

The information sources about IS events in IoTI are very traditional for any network environment as all the things in IoTI are connected by network channels (wired or wireless):

- Log files of IS management, control and monitoring systems;
- Information from separate domain controllers, proxy, DNS, web and mail servers, etc.;
- System log files of OSs and DBMSs;
- Log files of the application software, active network equipment (with flows and all connectivity records) and the used IPTs, including integrity check software, the IPT from unauthorized access, protection against malicious code, specialized tools such as endpoint IS thread detection solutions, FWs, IDPSs, security scanners and SIEM systems;
- Query results;
- Information from the specific physical access control devices, including television surveillance systems, access control systems and alarm system, and so on.

A few key verbal indicators of IS incident (also known as indicators of compromise) in IoTI's network were proposed. They are related to the typical activities or their combination associated with a specific remote network attack against IoTI's network. They can be described as follows.

- Unauthorized user on the network or shared credentials.
- Unauthorized access to confidential data, Personally Identifiable Information (PII) and financial data.
- Unauthorized internal host (client or server) connection to the Internet
- Excessive access from a 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.

Authorized licensed use limited to: ISRO Telemetry Tracking and Command Network. Downloaded on February 06,2025 at 09:03:07 UTC from IEEE Xplore. Restrictions apply.

- 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 a foreign country where there are no IoTI or to external hosts using non-standard ports or protocol/port mismatches.
- A single host/user account tries to login to multiple hosts within IoTI in a few minutes from/to different regions (a sign that the user's credentials have been stolen).
- The hosts, which are publically accessible or allocate in the IoTI's demilitarized zone (DMZ) communicate to some internal hosts that indicates leapfrogging from the outside to the inside and back, data exfiltration and remote access to IoTI's resources.
- Multiple alarms from a single host or duplicate events across multiple computers in the same subnet over a 24-hour period (such as repeated authentication failures).
- Repeated attack from a single source or on a single host.
- Service account access to the Internet or an unauthorized device.
- Network and vulnerability scanning and probing by internal hosts communicating with multiple hosts in a short time, by an unauthorized host or during an unauthorized time frame.
- Excessive traffic from a single source or to a single destination, outbound (e.g., web, email) or inbound (e.g., streaming, web).
- Missing or damaged files or appearance of new files that were not created by the internal users.
- Corrected or deleted logs from source or logging source stopped logging.
- Detection of typical well-known exploits.
- Detection of multiple infected hosts.
- Excessive scan timeouts from antivirus.
- After being cleaned, a system is reinfected with malware within a short time frame (a signal of a rootkit presence or persistent compromise).
- Excessive port blocking attempts from monitoring systems like antivirus.
- Unauthorized device on the network or device out of compliance (policies, patching, etc.).
- Multiple changes in a short time frame from administrative accounts.
- Unauthorized device (including IPT) configuration change.
- Anomalies in baselines for users' access and authentication, network, applications, suspicious activity, DoS, malware and so on.
- Another obvious signs such as failures, software malfunction, the repetition of some specific events, the wrong commands, incidental attributes, and inappropriate IoTI's network traffic's parameters.
- Suspicious events and processes, traffic to known vulnerable host, etc.

This list is not ranked. Any IoTI should implement its own IS incidents prioritization. For example, delivery of a malicious email is not as critical as active command and control between an intruder and an infected workstations and network devices. However, if mailboxes are provided, the consequences are clearly predictable – a loss of clients or business.

VII. First-generation SOCs' Limitations

The traditional SOCs with outdated for today rule-based SIEM systems have done well several years ago while protecting against the traditional attacks. But at present when the attack landscape is characterized by more targeted, smarter, stealthier, sophisticated and advanced techniques (like APTs and client-side attacks) we come to a conclusion that they cannot cope with increasing volumes of IS-related information in heterogeneous IoTI and they do not manage to keep control of the situation.

The following serious first-generation SOCs' limitations can be defined:

- Inability to work in the large-scale, globally deployed, heterogeneous, highly distributed and massively interconnected IoTI 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 centralized correlation rules processed on a single node, making scalability difficult, creating bottlenecks and single points 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 IoTI;
- Lack of online reaction to identified attacks; 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 derivated IS-related data known as big data;
- Inability to interpret data from the higher layers such as service or business impact view;
- Great number of false positives and false negatives as it main application area is to uncovering known or easy-to-detect IS threats;
- The old-practice first-generation SIEM systems that are used as a SOC core;
- Manual integration of IS technologies used.

Thus, the urgent and immutable modern requirements are full-visibility, behavior-based (detecting anomalies from a baseline of normal activity) approaches implementation and a heightened level of IoTI security that brings security intelligence with its actionable and comprehensive insight and predictive knowledge management to the forefront.

VIII. Discussion and Conclusion

ISIMP is one of the key management processes of any IoTI despite of its size and scope. The data received as a result of ISIMP are the inputs for another IS management processes and vice versa. For example, IS monitoring gives a lot of interesting information for ISIMP. ISIMP for IoTI is associated with the processing of large amounts of data, which requires a mandatory automation of routine operations. Qualitatively

Authorized licensed use limited to: ISRO Telemetry Tracking and Command Network. Downloaded on February 06,2025 at 09:03:07 UTC from IEEE Xplore. Restrictions apply.

designed and properly functioning ISIMP for IoTI reduces the number of IS incidents and limits damage caused by them and can be well automated by SOCs.

New reality of more frequent and sophisticated attacks and «hacking as a service» makes IoTI's network break-in more professional, accessible and dangerously effective. IoTIs must oppose this properly designed and centralized IS management systems, which combine stand-alone SIEM systems and IPTs, process massive flood of IS-related data and operate according to the unified and constantly controlled and modified IS policies and rigid legal ana regulatory requirements. Hence, to implement such an approach and to automate to the limit all the routine operations and IS incidents' response that do not require expert's decision-making it is urgent for any IoTI to set up an IS management center dealing with these challenges and being more advanced than a traditional SOC. To counteract to the network-level and more important higher-level IS events so called Security Intelligence Center (SIC) with an integrated architecture for protection against attacks provides full visibility and control and context-driven security intelligence in one place. Implementing SICs, we have a holistic in-depth view of their IoTI's «IS health» as SICs are capable not only to detect and recognize attacks, but also to effectively address IS threats before they cause harm and prevent IS incidents, constantly gathering and processing knowledge about actual network attacks.

To empower autonomy of IS incident management within one IoTI and to deepen its knowledge of the computing environment and IoTI in particular our further research is aimed at uniting together all advantages of SIC and Network Operations Center with their unique and joint toolkits and techniques in a unified Network Security Intelligence Center.

IX. Acknowledgement

This work was supported by Competitiveness Growth Program of the Federal Autonomous Educational Institution of Higher Education National Research Nuclear University MEPhI (Moscow Engineering Physics Institute).

References

[1] Recommendation ITU-T Y.2060. Overview of the Internet of things. International Telecommunication Union. 06/2012.

[2] 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. 2014. 2nd edition. 166 p.

[3] ISO/IEC 27035:2011 «Information technology -- Security techniques -- Information security incident management».

[4] ISO/IEC 27001:2013 «Information technology -- Security techniques -- Information security management systems -- Requirements».

[5] Cichonski P., Millar T., Grance T., Scarfone K. «NIST Special Publication 800-61 Rev 2: Computer Security Incident Handling Guide,» August 2012. URL: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf (access date 23.03.2016).

[6] Killcrece G., Kossakowski K.-P., Ruefle R., Zajicek M. Organizational Models for Computer Security Incident Response Teams. December 2003. URL: http://www.cert.org/archive/pdf/03hb001.pdf (access data 23.03.2016).

[7] 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. URL: http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6305 (access date 23.03.2016).

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

[9] Bace R.G., Intrusion Detection. Indianapolis: Macmillan Technical Publishing, 2000.

[10] Van Wyk K.R., Forno R. Incident Response, Sebastopol, CA: O'Reilly Media, Inc., 2001.

[11] Schultz E.E., Shumway R. Incident Response: A Strategic Guide to Handling System and Network Security Breaches, Sams, 2001.

[12] Northcutt S. Network Intrusion Detection (3rd Edition). Indianapolis: New Riders Publishing, 2002. 512 p.

[13] Spitzner L. Honeypots: Tracking Hackers, Addison-Wesley Professional, 2002.

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

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

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

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

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

[19] Bidou R. Security Operation Center Concepts & Implementation. 2005. URL: http://iv2-technologies.com/~rbidou/ SOCConceptAndImplementation.pdf (access date 31.01.2016).

[20] Security Operations Center: Building, Operating, and Maintaining your SOC. Cisco Press. 2015: URL: https://supportforums.cisco.com/sites/default/files/security_operations_center_9780134052014_ch_1_final__0.pdf (access date 23.03.2016).

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

[22] Rajnovic D. Computer Incident Response and Product Security, Indianapolis, IN: Cisco Press, 2011.

[23] Sanders C., Smith J. Applied Network Security Monitoring: Collection, Detection, and Analysis, Boston, MA: Syngress, 2013.

[24] Bejtlich R. Practice of Network Security Monitoring, San Francisco, CA: No Starch Press, 2013.

[25] ISO/IEC 27043:2015 «Information technology -- Security techniques -- Incident investigation principles and processes».

[26] Security Operations Center. URL: http://resources.infosecinstitute.com/security-operations-center/ (access date 23.03.2016).

Authorized licensed use limited to: ISRO Telemetry Tracking and Command Network. Downloaded on February 06,2025 at 09:03:07 UTC from IEEE Xplore. Restrictions apply.