# Going Beyond the Technical in SIEM



The majority of modern companies encounter information security challenges every day, ranging from external targeted attacks to internal leaks, despite using various information security approaches and tools. IT is rapidly evolving, in keeping with the threat landscape; but new approaches and tools mean new vulnerabilities. Violators are becoming smarter and faster. The classic confidentiality, integrity and availability (CIA) triad has not been enough to address these challenges, especially when information security incidents occur (i.e., the CIA triad was violated fully or partially).

Global analytical reports find a growing number of incidents annually and increasing incident sophistication.[1] In other words, incidents have happened, are happening and will be happening. For timely incident detection and deep forensics, it is necessary to expand information security abilities and the CIA triad, ensuring accountability. However, accountability creates millions of security events;[2] therefore, it is important to ensure effective security information and event management (SIEM)[3] within an information security management system (ISMS).[4]

This article addresses an existing imbalance between technical issues and process aspects related to SIEM. This gap is the root cause of some skepticism with and disappointment in SIEM.

## SIEM Process

Be aware that before implementing SIEM, it is necessary to establish the basis of the ISMS, which will include considering the global management commitment, asset inventory and categorization and risk assessment. The SIEM process can be implemented when the needed enterprise security tools are obtained and the process capability model level is no lower than the managed process outlined in COBIT® 5.[5]

The SIEM process consists of following a five-step cycle (see **figure 1**).

This SIEM approach is based on the plan-do-check-act (PDCA) cycle. This article focuses on the policy establishment step of the SIEM cycle.

## SIEM Policy Establishment

High-ranking management should demonstrate a commitment to the ISMS, including SIEM, by ensuring the SIEM policy is established and is compatible with the business direction, context and risk approach. Usually, the chief information security officer (CISO) prepares this internal policy and obtains the approval of all stakeholders. This policy should be mapped with existing internal policies, such as defining detailed event lists into standards and baselines for servers and network tools.

The SIEM policy should contain these basic components:

- Purpose of the policy
- Scope of the SIEM infrastructure
- Responsibilities of involved individuals
- Compliance

### Purpose

Purpose describes the need for a policy and should rely on and link to business tasks, objectives and context. There are many reasons for developing a SIEM policy. Some of the reasons include:

- Having a comprehensive IT security vision
- Developing incident detection
- Improving IT security forensics and analytics
- Establishing compliance

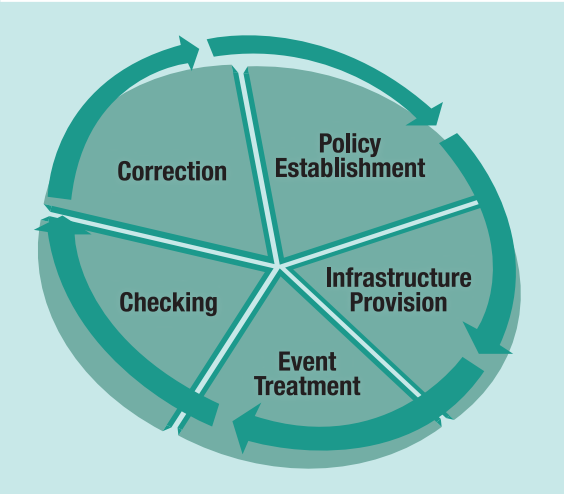
### Scope

Scope is the biggest part of the SIEM policy due to its description of the SIEM infrastructure. A SIEM infrastructure is more than just the SIEM system. It is a common misconception that a SIEM system is the essential component for SIEM infrastructure. The SIEM system is a technological solution and is just a component of the SIEM infrastructure. A SIEM infrastructure consists of different event sources, event storage, analysis tools and a monitoring console and also includes external information providers, e.g., McAfee Global Threat Intelligence, RSA FirstWatch and Kaspersky Security Intelligence Services. Event sources are an essential component

**Do you have something to say about this article?**
Visit the Journal pages of the ISACA web site *(www.isaca.org/journal)*,find the article and click on the Comments link to share your thoughts.

**Aleksandr Kuznetcov,** CISM
Is head of the information security department at the research and development center at Vulkan LLP. In this capacity, he leads the security information and event management (SIEM) implementation team. He has 10 years of experience in information security and five years of experience in SIEM. He is an active author and public speaker on his areas of expertise. He is also pursuing a postgraduate degree at Financial University (Moscow, Russia).

**Figure 1—The Steps of the SIEM Cycle**




**Source:** Aleksandr Kuznetcov. Reprinted with permission.

of SIEM infrastructure as the event source puts data into audit trails (i.e., registered events). Without registered events, a SIEM system is useless.

An event source is any software or fireware (a set of software and hardware). This can include:

- Firewalls (FW)
- Host/network intrusion detection/protection systems (IDS/IPS)
- Virtual private network (VPN) tools
- Unified threat management (UTM) systems
- Certification authority (CA)
- Encryption tools
- Endpoint security tools
- Antivirus (AV) tools
- Vulnerability scanners (VS)
- Data loss prevention (DLP) systems
- Identity and access management (IAM) systems
- System software (e.g., operation system, hypervisor)
- Application software (e.g., database management system, web server)

There are two main criteria that determine if a piece of equipment is the event source:

- Logging ability
- Ability to provide access to log data

If the first criterion is not possible, the equipment in question is not an event source. If the second criterion is not possible, the equipment is an isolated event source.

The main component of event sources are security tools, which are enterprise-level solutions that comply with the two previously discussed main factors (i.e., logging ability and ability to provide access to log data). Tools such as FW, IDS/IPS or UTM are network security tools.

There is a separate type of event source that supplies network packets. This type of tool includes Switched Port Analyzer (SPAN) ports, Test Access Point (TAP) solutions and sniffers. Network packets may be more useful than log data.

Brian Girardi, vice president of product architecture and research at RSA, said, “We need more complete data sources and visibility into networking data, which means the way we keep, manage, process and model data must change. We need to make it more consumable—not just more data, but better data.” To make data more consumable, the following questions should be considered:

- Where are data collected?
- What is collecting data?

The following steps can provide enterprises with some direction when answering the previous questions:

- Segment the network in consistency with asset groups and critical levels, i.e., define trusted zones (e.g., internal segment, preproduction segment) and critical zones (e.g., the payment card industry segment, demilitarized zone).
- Define interconnection points between zones.
- Data should flow relatively freely within trusted zones, whereas data flowing in and out of the trusted zone (interconnection points) require more control.



Therefore, data should be collected:

- Within trusted zones at the basic level (logs)
- Within critical zones at the advanced level (first, logs; second, network packets)
- Into interconnection points at the advanced level (first, network packets; second, logs)

When discussing what is being collected, remember that the first principle of gathering is that collecting all data is not the main goal of SIEM. Collected data must be valuable, and unused data are not required and should be discarded. Unused data are of no value and waste the time of the SIEM team. Remember that collection from a 100 Mbps line (network packets) equates to 1 terabyte (TB) of storage per day. Not all organizations are prepared to spend enough to develop this kind of storage capacity. To better manage this large storage requirement, consider the following:

- Become familiar with baseline and normal events (create a business-day profile, define top of services, sources and destinations).
- Filter out known good and unwanted network traffic (allowed by information security policies), i.e., reduce the amount of information, but do not just drop or filter it because it takes up space.
- Focus on the critical security information. This can provide better visibility into unknown and untrusted data.
- Focus on the places where there are no information security controls.
- Periodically (e.g., monthly) review defined baselines and profiles.

**Responsibilities**

While senior management should retain overall responsibility for the SIEM policy, a SIEM process owner should be appointed. This process owner does not have to be the chief information security officer (CISO). Senior management should define SIEM team structure.

**Compliance**

Compliance defines how to judge the effectiveness of a SIEM policy (i.e., how well it is working) and what happens when this policy is violated (the sanction). Sometimes, metrics and key performance indicators are described in this portion.

## Conclusion

The SIEM has become the core of an ISMS and security operation centers (SOC), but it is unwise to rely on just the technical aspects of SIEM. The SIEM policy is essential for ensuring effective SIEM within an ISMS. The time used for SIEM policy development is worthwhile; it will save effort in future steps. The biggest part of the policy—scope—deserves special attention, and it is important to remember that the basis of SIEM infrastructure is event sources, not the SIEM system.

## Endnotes

1 PricewaterhouseCoopers, *The Global State of Information Security Survey 2016*, 2015, *www.pwc.com/gsiss2015*

2 A security event is a change in or retention of the status, which has implications for IS, management, the health of the component(s) of IT infrastructure and/or ISMS of a company. It also affects the audit trail (file, database table or some other location) information for this event.

3 SIEM is a part of the ISMS of a company, including technological components, processes and staff.

4 ISMS is a part of the overall management system of a company, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve IS.

5 ISACA, COBIT 5, USA, 2012, *www.isaca.org/cobit*