cloud security alliance℠

*SecaaS Implementation Guidance*

# Category 7 // Security Information and Event Management

September 2012

# Contents



 

 

# Foreword

Cloud Computing represents one of the most significant shifts in information technology many of us are likely to see in our lifetimes. We are reaching the point where computing functions as a utility, promising innovations yet unimagined. The major roadblock to full adoption of Cloud Computing has been concern regarding the security and privacy of information.

Much work has been done regarding the security of the cloud and data within it, but until now, there have been no best practices to follow when developing or assessing security services in an elastic cloud model—a model that scales as client requirements change.

One mission of the Cloud Security Alliance is to provide education on the uses of Cloud Computing to help secure all other forms of computing. To aid both cloud customers and cloud providers, the CSA SecaaS Working Group is providing Implementation Guidance for each category of Security as a Service, as delineated in the CSA's SecaaS Defined Categories of Service. Security as a Service was added, as Domain 14, to version 3 of the CSA Guidance.

Cloud Security Alliance SecaaS Implementation Guidance documents are available at https://cloudsecurityalliance.org/research/working-groups/security-as-a-service/.

We encourage you to download and review all of our flagship research at http://www.cloudsecurityalliance.org.

Best regards,

| | | |
|---|---|---|
| Jerry Archer | Alan Boehme | Dave Cullinane |
| Nils Puhlmann | Paul Kurtz | Jim Reavis |

The Cloud Security Alliance Board of Directors

# Letter from the Co-Chairs

Security as a Service is a specialized area categorized two years ago as growing rapidly and in unbound patterns. Vendors were struggling. Consumers were struggling. Each offering had its own path. We felt it was urgent to address the needs and concerns common to the implementation of Security as a Service in its many forms.

The Defined Categories of Service helped clarify the functionalities expected from each Category. In this series, we hope to better define best practices in the design, development, assessment and implementation of today's offerings.

We want to thank all of the many contributors worldwide who have worked so hard to produce these papers providing guidance for best practices in Cloud Computing Security. Many have been with the Security as a Service Working Group since the beginning; many others joined in this effort. Each has spent countless hours considering, clarifying, writing and/or editing these papers. We hope they help move forward toward those unimagined innovations.

Sincerely,

Kevin Fielder and Cameron Smith
SecaaS Working Group Co-Chairs

# Acknowledgments

Co-Chairs

Jens Laundrup, Emagined
Wendy Cohen , GBT Technologies
Atul Shah, Microsoft

Contributors

Andrea Bilobrk, Cloud & Virtualization Security Strategist,  Canada Cloud Network
Moshe Ferber , Machshava Tova
Robert Gutcho, Symantec
Bernd Jäger, Colt
Yale Li, Microsoft
Roshan Sequeira, ISITRoshan Sequiera, ISIT

Peer Reviewers

Andrea Bilobrk, Cloud & Virtualization Security Strategist, Canada Cloud Network
Rizwan Ahmad
Phil Cox, Director of Security and Compliance, RightScale
Moshe Ferber, Machshava Tova
Andrew Hay, Chief Evangelist, CloudPassage, Inc.
Bernd Jäger, Colt
Hament Mahajan, Juniper Networks
Anish Mohammed, Accenture
Karthik Murthy, Advanced Technology Services
Jean Pawluk
Paul Swinton, Symantec

CSA Global Staff

Aaron Alva, Research Intern
Vicki Hahn, Technical Writer/Editor
Luciano JR Santos, Research Director
Kendall Scoboria, Graphic Designer
Evan Scoboria, Webmaster
John Yeoh, Research Analyst

 

# 1.0 Introduction

Tremendous professional judgment and experience must be applied in the architecture, engineering, and implementation of Security Information and Event Management (SIEM), to ensure that it logs the information necessary to successfully increase visibility and remove ambiguity surrounding security events and risks that an organization faces. Providing SIEM as a service under Security as a Service (SecaaS), the provider must be able to accept log, event and flow information from a diverse set of current and legacy customer devices, conduct information security analysis, correlation, and support incident response activities from a wide variety of sources. By providing flexible, real-time access to SIEM information, it allows the party consuming the SIEM service to identify threats acting against their environment, cloud or other. This identification then allows for the appropriate action and response to be undertaken to protect or mitigate the threat. This simple step of increasing visibility and removing ambiguity helps the organization understand the current vulnerabilities and gaps, increase the effectiveness of the controls deployed and improve the security posture of the organization as a whole.

This document provides guidance on how to evaluate, architect, and deploy cloud-based SIEM services to both enterprise and cloud-based networks, infrastructure and applications. The guidance addresses the leveraging of cloud-based SIEM services in support of cloud environments, both public and private, hybrid environments, and traditional non-cloud environments. While this document addresses SIEM as a cloud service, it does not preclude a hybrid environment for enterprises that have traditional SIEM deployments where the SIEM cloud service supplements.

## 1.1 Intended Audience

The target audience of this document is primarily IT security managers, technical architects and systems managers who are responsible for monitoring and auditing their organization's infrastructure and applications. SIEM data can be used for general monitoring as well as security monitoring and auditing. In addition to technical staff, other staff such as IT generalists, auditors and compliance managers may benefit. Technically proficient C-level board members such as CTOs, CISOs, and CIOs may find this a useful reference, providing an overview of cloud-based SIEM services and the areas that should be addressed if they are considering implementing/consuming such a service.

Section 2 is intended as a high level overview of SIEM functions and implementation options. It addresses several key functionalities for which SIEM can be leveraged, and it touches on less traditional deployments that can be implemented in specific markets where regulatory or other compliance requires it. The intended audience includes executive and senior leadership responsible for IT and security operations, compliance officers, and other decision makers within an enterprise. The material is written for executive-level discussion and indicates a baseline for best practices in implementation and design of security services in the cloud.

Section 3 details the considerations and concerns that should be part of the decision-making conversation, whether by an architecture team, auditing team, or within the context of a purchasing decision. The section is written for those who are implementing, integrating with, or performing a technical evaluation of cloud-based SIEM. This section also is well suited for auditors to help them understand typical services and capabilities that may be implemented for cloud-based SIEM deployments.

Section 4 is a technical discussion. The section is divided into two subsections, the first addresses architectural considerations for network architects and the second addresses security analysts' considerations.

Section 5 contains links to trusted sources of information regarding SIEM and SecaaS and references used in the creation of this document.

## 1.2 Scope

This guidance will cover generic (non-industry specific) implementations only at this time. While some applications discussed herein may apply only to a few vertical markets, the examples and illustrations likely will refer to a specific industry. Despite this, the guidance should be regarded as neutral in all aspects, and any inference to a specific vendor or industry is purely accidental. This guide will not address specific requirements that individual SecaaS providers may have in order to establish the service.

# 2.0 Requirements Addressed

## 2.1 SIEM Functionality

Security Information and Event Management (SIEM) systems are designed to accept log event and flow information from a broad range of systems, including traditional security systems, management systems, or any other systems which provide a relevant data output that, when correlated and analyzed, is relevant for the enterprise. Traditional security systems include technologies such as firewalls, intrusion detection/prevention systems, anti-malware systems, and others that are deployed at both the host and network level. Management systems include Active Directory (AD), Identity and Access Management (IAM) systems, Network Management Systems, and others. Less traditional sources of data can include access control systems, video monitoring systems, elevator control systems, HVAC systems, telephone switches (VOIP or otherwise), email, DLP, etc. Any type of SIEM is of no value if it is only collecting data from a single device or if it only collects a single specific type of event from the enterprise, since it defeats the purpose of correlating events. The efficacy of the output relies on having a broad set of data.

Applications and devices designed to achieve objectives such as protecting the perimeter, managing access rights, and securing against challenging end point vulnerabilities are often mutually exclusive in terms of their effectiveness, and offer no centralized oversight to the critical threats that can pose the greatest risks to a cloud infrastructure. A SIEM can help gain centralized visibility, leverage the value of existing investments and prepare for potential threats that could compromise their business-critical information assets. A SIEM establishes an early warning system to take helpful preventative actions. An effective early warning system detects threats based on a global perspective and provides in-depth information about them. It also recommends measures that can be taken to protect the cloud infrastructure. As part of the implementation of a SIEM solution, tuning is performed to reduce false positive alerts and ensure that the device provides relevant information to each specific environment.

The information collected by the SIEM is typically aggregated (put into a single stream) and normalized (translated into a standardized format) by the SIEM to reduce duplicates and to expedite subsequent analysis. It is then correlated between data sources and analyzed against a set of human defined rules, or vendor supplied or security analyst programmed correlation algorithms, to provide real-time reporting and alerting on incidents/events that may require intervention. The subsequent data is typically stored in a manner that prevents tampering to enable their use as evidence in any investigations or to meet compliance requirements.

The SIEM provides maintenance and authoring of correlation rules and allows system rules to cover a multitude of conditions. In addition to condition action rules, a SIEM often supports rules that can execute based on arbitrary conditions as well as anomalous behavior. An example of such a rule is a negative condition rule, where the absence of an event over a period of time executes a rule, such as a back-up process that misses a scheduled routine.

Traditional “on-premises” SIEM implementations often take considerably more effort and time to implement successfully than businesses envision. SIEM projects, especially in SMBs or larger enterprises with limited IT

 

expertise, often fail to evolve past the planning phase or are only partially successful. This is often because the required tuning and validation of SIEM events requires a specialized skill set and monitoring during the implementation stages. The promise of SIEM provided from a cloud-based service can provide a scalable, fully managed SIEM service that the customer can leverage and integrate with public cloud, private cloud, and on-premise systems and infrastructure. It is important to note, however, that many of the same requirements still exist, and the business needs to ensure that adequate resources are devoted to the initial set-up and subsequent monitoring and maintenance of rules.

SIEM in the cloud enables the customer to test the service and gradually deploy and integrate it with their systems, while paying only for the services they are using, rather than having to purchase a full SIEM solution up front. Some clients may opt to leverage cloud-based SIEM services to monitor their systems in the public cloud space while using their on premises SIEM implementation for their private cloud and traditional systems implementations. In both cases, customers can opt to have the SIEM either simply hosted, with the customer providing the monitoring of the log information, or fully managed, where the cloud SIEM provider performs the monitoring and alerting services to the customer.

## 2.2 Business Drivers

SIEM capabilities are highly flexible and are capable of addressing multiple needs within organizations. These drivers can be more practical as in reducing the efforts by an enterprise to gather network and system usage information for network architectural purposes, to risk management and security, and also regulatory and compliance uses. While each of these may seem unique and unrelated, they all rely on the same organizational data.

### 2.2.1 Log Data Management

A SIEM provides, among other things, log retention and retrieval capabilities through flexible querying and reporting options that furnish auditors and other related stakeholders the information they need. It can be leveraged to manage the ever growing volumes of log data that are needed to show compliance with legal and industry rules, along with best practices. A properly configured SIEM can search the proverbial haystack for the needles and find the data necessary in relatively short order. This can include searches through archived data that may not reside immediately within the SIEM system's infrastructure but may be located in a storage cloud. Most enterprise class SIEM also are able to automatically sort, segregate and dispose of data based on multiple retention schedules in order to discard excess information after its retention period while maintaining data and event summaries for longer time periods.

### 2.2.2 Risk Management

A SIEM produces executive, technical, and audit-level reports that are highly effective at communicating risk levels and the security posture of the cloud infrastructure. SIEM technology is being used not just to analyze data after an incident, but also to perform near real-time detection, quickly followed by meaningful event management and subsequent forensic examination. SIEM is a differentiator is in its capability to quickly sift through a sea of security and log data and detect behaviors in the enterprise that indicate malfeasance. This

includes not just traditional threats presented by “hackers” on the web, but can include Advanced Persistent Threats (APT), insider threats, and malware threats to the network. It also can be used to detect other forms of questionable behavior such as insider trading, monitoring identity and access activities, unauthorized personnel looking at health records in hospitals, fraud detection, privilege escalation, and more.

Newer SIEM logic capabilities include the ability to identify the threats and vulnerabilities in cloud infrastructures, and provide remediation steps to address those threats in close to real time. This helps the enterprise mitigate the added threats and vulnerabilities that come with migration of systems into the cloud infrastructure.

### 2.2.3 Regulatory and Compliance Requirements

There is a host of regulatory requirements that SIEM can help organizations address. Regulatory needs include local, state or provincial laws in addition to national and international rules and laws that businesses must show adherence with. Additionally, industry specific rules and best practices that enterprises either want or must comply with, and in some enterprises, internal policies and requirements must also be considered. They can be privacy laws such as the European Protection Directive, or the Personal Information Protection Law in Japan, banking rules such as those put forth by the Financial Services Agency (Japan), healthcare rules such as HIPAA (US), international rules such as PCI imposed by the payment Card Industry, or simply enterprise policies on matters such as Acceptable Use Policies or data retention rules. In the past, organizations were required to prove annual or biennial adherence to such rules, but the trend is for businesses and agencies to demonstrate continuous compliance – a task that is reduced in complexity by employing dynamic systems such as SIEMs. Many businesses may also find that it is less costly to invest in a SIEM solution, cloud-based, traditional, or hybrid, than the cost of deploying and maintaining homegrown tools or regular assessment by major auditing firms or a large team of internal auditors. Compliance, specifically with regards to the management of an organization’s log retention requirements, remains the most common justification for new SIEM implementations. For industries with compliance requirements, particularly those with geographical restrictions on data movement, the location of log data should be verified to ensure it does not invalidate compliancy.

## 2.3 Incidents and Events

A great number of security, compliance and operational event sequences can be automated by a SIEM in order to help reduce risks within the enterprise. A SIEM generated incident typically creates a workflow to facilitate the containment, eradication, and recovery process. It can include the initiation and tracking of checklists for individual incidents to ensure all necessary actions are being taken to minimize and contain the incident in a standardized, policy-driven manner. This workflow is often feed a third-party ticketing help-desk solution, wherein a ticket or series of tickets is created, processed, and tracked back into the system. If these events require additional scrutiny by regulatory or law enforcement agencies, a SIEM can generate forensically sound data subsets with time stamps that can be exported and analyzed independently by the SIEM or third-party forensic or investigative tools.

## 2.4 Performance Requirements

When determining what level of security to contract out to a SecaaS vendor, the leadership needs to evaluate and consider the consequences of each decision. Considerations include but are not limited to questions regarding:

- Who is responsible for monitoring alerts locally and at the vendor?
- What alert responses can the vendor do, what does the enterprise IT staff do? The delineation of duties has to be spelled out clearly so that both the enterprise and the vendor have a clear understanding of what the expectations are and how hand-offs are accomplished.
- How does the vendor gain access to respond to an alert? If the SecaaS SIEM vendor is expected to respond by actively protecting the enterprise cloud, they will need access and administrative right to it. Should they be expected to protect the enterprise network, they will need administrative access to the enterprise network.
- What actions will the vendor be allowed to take? Granting administrative access to the vendor for the purposes of defending the network grants them unfettered access to the network and its components.
- How much access does the vendor want/need? How much is the enterprise willing to give them?
- Graphical event overview (a map of the network and the issues) – This type of visual display enhances the abilities of analysts to respond to breaches and infections by providing a quick look to determine where problems lie and how they are progressing or spreading. Will the vendor provide one to the analysts and network personnel combating a breach or infection?

## 2.5 Service Level Agreements

Service Level Agreements (SLAs) for cloud services are typically poorly written and favor the SecaaS SIEM provider more so than the user. The providers typically write the SLAs, so it is incumbent upon the enterprise senior leadership and the legal staff, to ensure the rights and needs of the enterprise are best served. Some areas to carefully consider are:

- Provisions for delegated and/or joint control must be described in detail in the SLA. This is particularly important if the provider is tasked with monitoring and acting upon incidents which will then be worked by analysts of both parties.
- Requirements for availability, handling, storage, and disposal of proprietary and personally identifiable information must be specifically stated, including geographical location of log and security data if required for compliance.
- Any requirements for encryption of data at rest and/or in motion must be delineated in detail including who holds and/or controls the key materials.
- Detailed requirements for incident response, business continuity and disaster recovery procedures and operations must be spelled out.
- Third-party audit arrangements must be made explicit. This is particularly important if law enforcement agencies require access to the data collected by the provider. If the data resides in a different continent, you may bear all the costs of the agency to travel to the location and collect it.

- Notification procedures if the SecaaS SIEM provider is served with a legal dictate to provide access to data that may include your data.
- The requirement to ensure that the data collected by the SecaaS SIEM provider be collected and stored in a forensically sound manner that meets the legal requirements of your particular country and regulatory rules.
- Availability requirements, to include the communications channels between the SecaaS SEIM provider and you including notification window times for each alert severity.
- Privacy and security of the data
- If and how access to the data is arranged in the event it is needed for forensic purposes. Most providers will grant you access to your own data only but not to affiliated data that may reveal additional information that could be useful in an investigation.
- The ability to audit the SecaaS SIEM vendor and their facilities. This may be particularly important if your enterprise needs a SSAE 16 or SAS 70 audit, a PCI audit or other audit in order to demonstrate your ability to comply with a rule or regulatory requirement.
- Performance Guarantees and warranties should a SecaaS SIEM provider acts negligently or even maliciously.

Ultimately, an organization's contracts and/or legal office will be responsible for critically examining and approving terms of any SLAs for the protection of the enterprise. It is incumbent upon the senior leadership to ensure that all potential issues are raised, addressed and understood up front. The signee must thoroughly understand the downsides of and worst cases in cloud-based SecaaS SIEM to help ensure that appropriate provisions are included in the SLA. Ideally, the providers should include indemnity clauses, such that if they make mistakes that are costly to their customers, the SecaaS SIEM provider will have to provide monetary compensation to cover the harm done. Most providers will not want to do this but it is in the best interests of the enterprise to ensure that all possible protections are in place and that there are compensation clauses for mistakes and loss of service that results in costs to the enterprise. Any "hold harmless" clauses in a SecaaS SIEM contract or SLA should automatically be eliminated.

# 3.0 Implementation Considerations and Concerns

## 3.1 Considerations

### 3.1.1 Implementation Considerations

In considering a SIEM solution, it becomes important to consider the problem(s) being addressed from an enterprise perspective to ensure it does not morph into an undefined and costly project that fails to meet the business requirements. This should include documenting in detail each of the problems that need to be addressed by the solution and the beneficiary of the solution. It should also include the perspective of how this benefits the corporate department (security, risk, compliance, fraud, Human Resources, Audit, etc.) and how responses to actions generated will improve processes over current solutions. This should include specific use case requirements.

Other implementation items to consider include reviewing the offering and making sure it fulfills all the business requirements. Most SecaaS SIEM providers will limit their offering in several ways so an evaluation period may be an important step. When evaluating SIEM as a service offering, customer should check the following:

- **Monitored devices** – Most providers market their offer based on number of monitored devices. There could be a difference between how their SIEM product counts device. Try to list all the devices that should be included. Some SecaaS SIEM vendors will count a log server as a single device whereas others will base their count on how many devices report in to the log server.
- **Supported device vs. unsupported** – Some SecaaS SIEM providers will charge extra for unsupported devices or devices that have unique log formats. Insist on viewing support matrix and understand how it will affect the cost. If you are working with a virtualized environment, ensure that the SIEM can see within each individual virtual machine and track changes within the hypervisor.
- **Number of reports / rules / EPS (event per second)** – Some SecaaS SIEM provider will charge extra on additional reports / events. Make sure that you are covered.
- **Standard vs. custom rules** – Some SecaaS SIEM vendors will charge a per-rule fee for each rule invoked. They may also charge extra for custom rules or rules that the enterprise create ad hoc to examine a problem. This can become very expensive if the device is not tuned to your environment properly.
- **Number of dashboards or/and users** – The number of dashboards and services made available for self service and customer internal use of SIEM should be clearly defined. There is sometimes a “Per Seat” charge for the dashboards and often the internal use of the SIEM is discouraged by charging extra for that service.
- **Log retention, log access and log storage** – Make sure the offering helps you address your regulatory requirements; particularly where logs are stored and how access is controlled. Also, make sure that once the logs are deleted in accordance with your retention specifications. If the retention policies require active and then long-term retention, make sure that the vendor provides an option to transfer the logs to the enterprise in a standard (non-proprietary) format for internal long term retention.

## 3.1.2 Legal Considerations

Internet monitoring in the workplace often pits employers and employees against each other because both sides are trying to protect personal interests. Employees want to maintain privacy while employers want to ensure company resources are not misused. Since SIEM collect log data that may show many different traffic streams, server logs, e-mail activity, surfing habits and more, enterprises should document and maintain ethical monitoring policies and avoid indiscriminate monitoring of employees' online activities whether it is inadvertent or otherwise. It could require changes to corporate policies as well as employment and union contracts in some instances.

A secondary legal concern is that when data is collected, it may then create legal or political ramifications to having the data and failing to take action on it. Realizing that not every bit of data can be thoroughly analyzed, an enterprise must be ready to respond to questions as to why they had the data but did not act upon it. In some situations in some places, not having the data may be more desirable than having the data and then failing to act upon it.

It is always best to seek counsel to address any legal concerns that may arise.

## 3.1.3 Ethical Considerations

Security analysts and other personnel assigned to monitor the SIEM feeds may be able to view e-mail activity, social media, and more in the performance of their duties. While the legal issues must be addressed, there is a larger ethical consideration that must also be considered. The employees' privacy in these areas will be compromised as it becomes visible to the analysts. The analysts monitoring the information must be made aware of privacy and confidentiality expectations as well as the employees being monitored should be able to expect some level of privacy and confidentiality regardless of what the legal muster and enterprise policies may be.

## 3.1.4 Cloud SIEM versus Hybrid SIEM

As with any solution, there are several ways that a SecaaS SIEM solution can be implemented. It can be a stand-alone solution in the cloud that monitors the enterprise traditional data center assets, private/public/hybrid cloud assets, or both. A pure SecaaS SIEM solution would rely solely upon the provider to monitor all the moni9tored systems (see Figure 1).

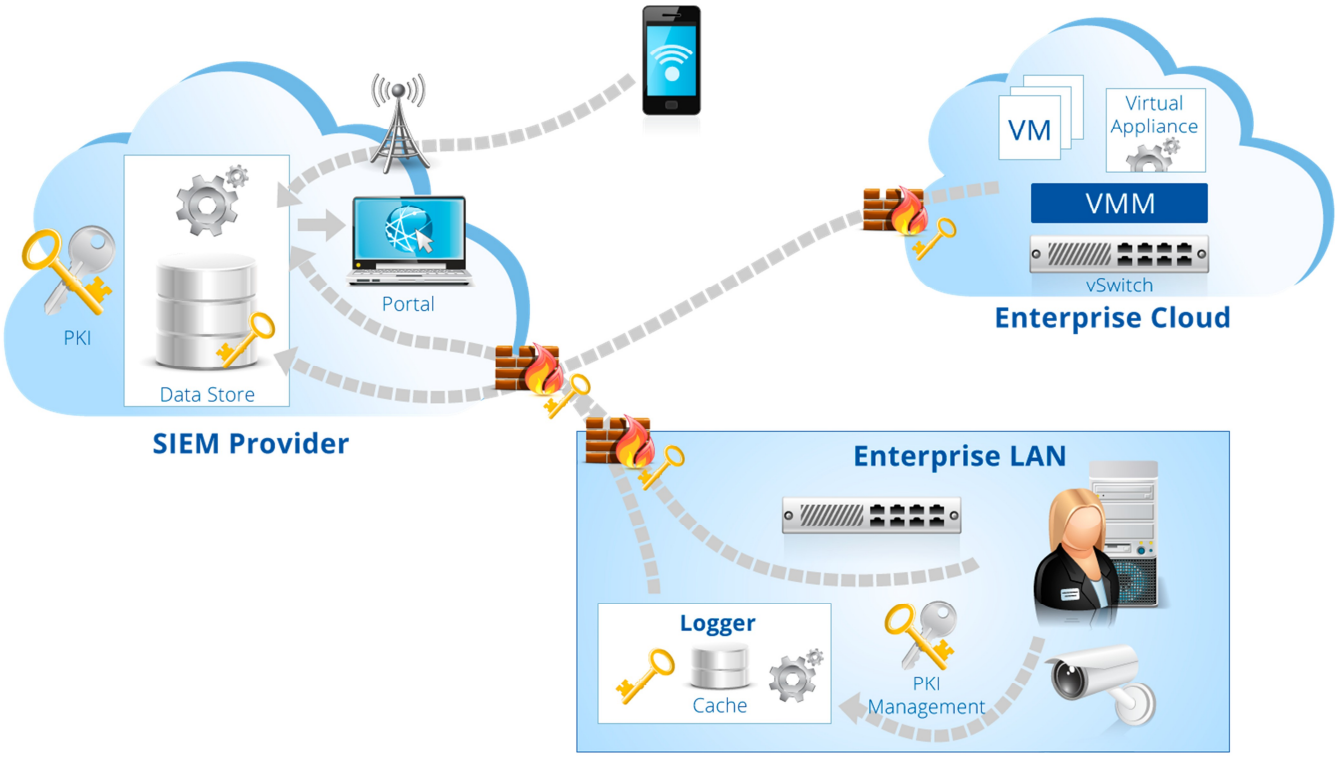


*Figure 1: SecaaS SIEM Solution*

Another option is to enlist the services of a SecaaS SIEM provider to monitor the enterprise external or cloud assets while using a traditional SIEM to monitor the traditional and private cloud infrastructures (see figure 2). These can then be linked by forwarding the SIEM traffic from the SecaaS SIEM to the "Master" SIEM in the enterprise network for overall analysis and monitoring. The advantage of doing so it that the enterprise minimizes its exposure of information to the SecaaS SIEM provider, and if the enterprise connectivity to the internet is broken, they still have the enterprise SIEM to collect, analyze and respond to an incident while the SecaaS SIEM continues to monitor the enterprise cloud assets.

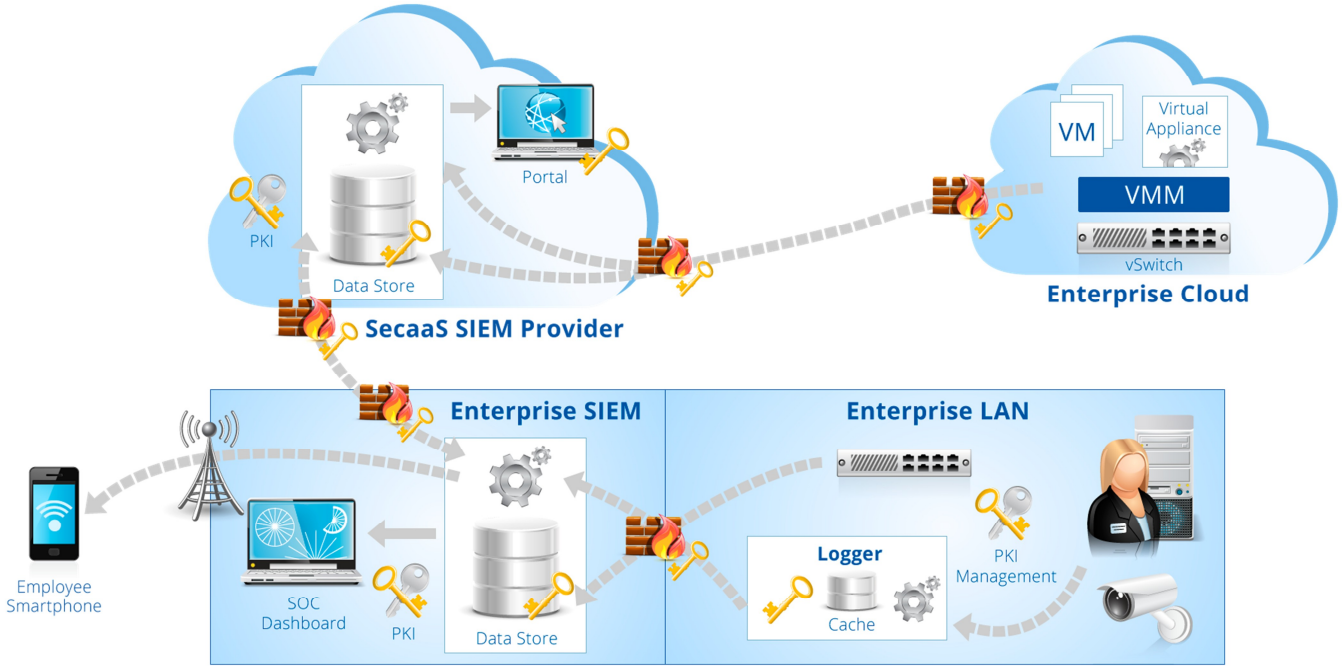


*Figure 2: Hybrid SIEM Architecture*

The architecture selected should be based upon the business needs and the network architecture that the SIEM architecture has to support.

## 3.1.5 Information Sharing

When engaging the services of a cloud-based SecaaS SIEM provider, whether exclusively or in a hybrid configuration, the provider will have access to the information gathered and may opt to aggregate your data with data from other clients in order to maximize their visibility of attacks and issues in their own environment and in the greater web. This same information is what their analysts will use to help you protect your enterprise and data regardless of its location. By the provider gaining access to the data, they have the ability to examine log feeds that may contain corporate information that is private, confidential, or classified. How the data is collected, used, and potentially shared by the SecaaS SIEM vendor needs to be considered. The data collected by the SIEM reveals a great deal about the weaknesses and vulnerabilities of an enterprise, it can be used by hackers to help them determine the best method of attacking a network, and it can be used real-time to guide them past enterprise defenses and alert them if they have been detected.

Organizations usually have the ability to obfuscate what information is written to disk without dramatically impacting the SecaaS SIEM provider's ability to manage alerting from a global perspective. Similarly, some technologies may allow users to selectively send information to their SecaaS SIEM after removing sensitive details from the log files.

## 3.2 Concerns

The major concern of a cloud-based, SecaaS SIEM infrastructure is that when the infrastructure is under attack, a poorly architected solution means that the analysts and senior management lose the security provided by the SIEM infrastructure. An enterprise under a distributed DOS attack will most likely lose connectivity, response, and remediation data from the SIEM if the SIEM systems share the enterprise network data flows. The response to the incident is only as good as the security information it is based upon. Therefore, alternate routes for the security systems should be considered.

Deperimeterization of security controls, including the SecaaS SIEM, is what is creating the most confusion in security today. With the integration of public cloud-based services, private cloud services, traditional networks, and the mobile workforce, a well layered and segmented approach needs to be created in order to support a SIEM system. When the enterprise network is under attack or failing, the SIEM system infrastructure needs to be solid so that the incident response teams can rely on the data to protect and remediate.

Disaster Recovery and Business Continuity (DR/BC) is another area of concern for network and security teams. Often, the data within the SIEM system holds the clues to what happened and what problem that needs to be addressed before the enterprise can be returned to normal. Furthermore, consideration needs to be given to when the data feeds for the SIEM system fail and what happens to the data at that time. Most regulatory driven systems require that a back-up system exist to gather the information so that when the security systems come back on line, a proper forensic examination can occur with backup log feeds.

Time standards and delays must be addressed in the architecture. Most SIEM systems require a standard time source and will timestamp all data as it arrives. If the SIEM system includes both a SecaaS SIEM and a traditional SIEM, these timestamps must be synchronized to the same time standard to ensure that the two logs (a local and a SecaaS SIEM vendor log) can be combined in a sound forensic manner for analysis. This is not an impossible task since time delays between correlation at the vendor site and the return alert receipts along with timestamps in the network logs can provide the information necessary to accomplish this.

Security of log data in transit and the security of log data at rest also need to be a major concern for the architects. Encrypted data is useless if the keys are somehow corrupted or lost. The security of logs at the vendor should not be protected by the same keys as those within the enterprise, and all the transactions between the vendor and the enterprise needs to be accomplished using keys that are regularly.

# 4.0 Implementation

The integration of a SIEM, regardless of whether it is a purely SecaaS solution or a hybrid solution, needs to be integrated into both the network architecture and the operational architecture. Implementation into the physical architecture without integration into operational and policy architectures can render the SIEM implementation of no use to the organization. The architectural and operational implementation considerations are addressed in this section but no attempt is made to address policy issues, as they are highly regionalized and vary widely depending on the industry they serve.

## 4.1 Architecture Overview

The architectural integration of a cloud-based SIEM or hybrid SIEM should be considered carefully. The key to a successful architecture is in understanding how the enterprise operates as well as crucial business patterns and assets. Other important knowledge is to understand what the identified business drivers for the SIEM system is so that the architecture is optimized to support them. The approach documented herein is intended to address any SIEM system and should be used every time a new problem that the SIEM system is designated to solve is identified. It does mean effort has to be applied, but it also means you will have objective

> **NOTE:** For the purpose of the architectural and technical discussions, the SIEM will be referred to generically as the SIEM or the SIEM system in lieu of attempting to define it as a cloud-based SIEM, traditional SIEM or hybrid SIEM.

### 4.1.1 Architectural Planning

In order to develop a successful plan, the architectural goals should ensure that the detection phase in the defended framework is made stronger by increasing the breadth and accuracy of detection. It also should support other phases by providing intelligence for decisions in protection, response, and recovery and ensure the best possible defense by optimizing security management within and across enterprise and into the cloud.

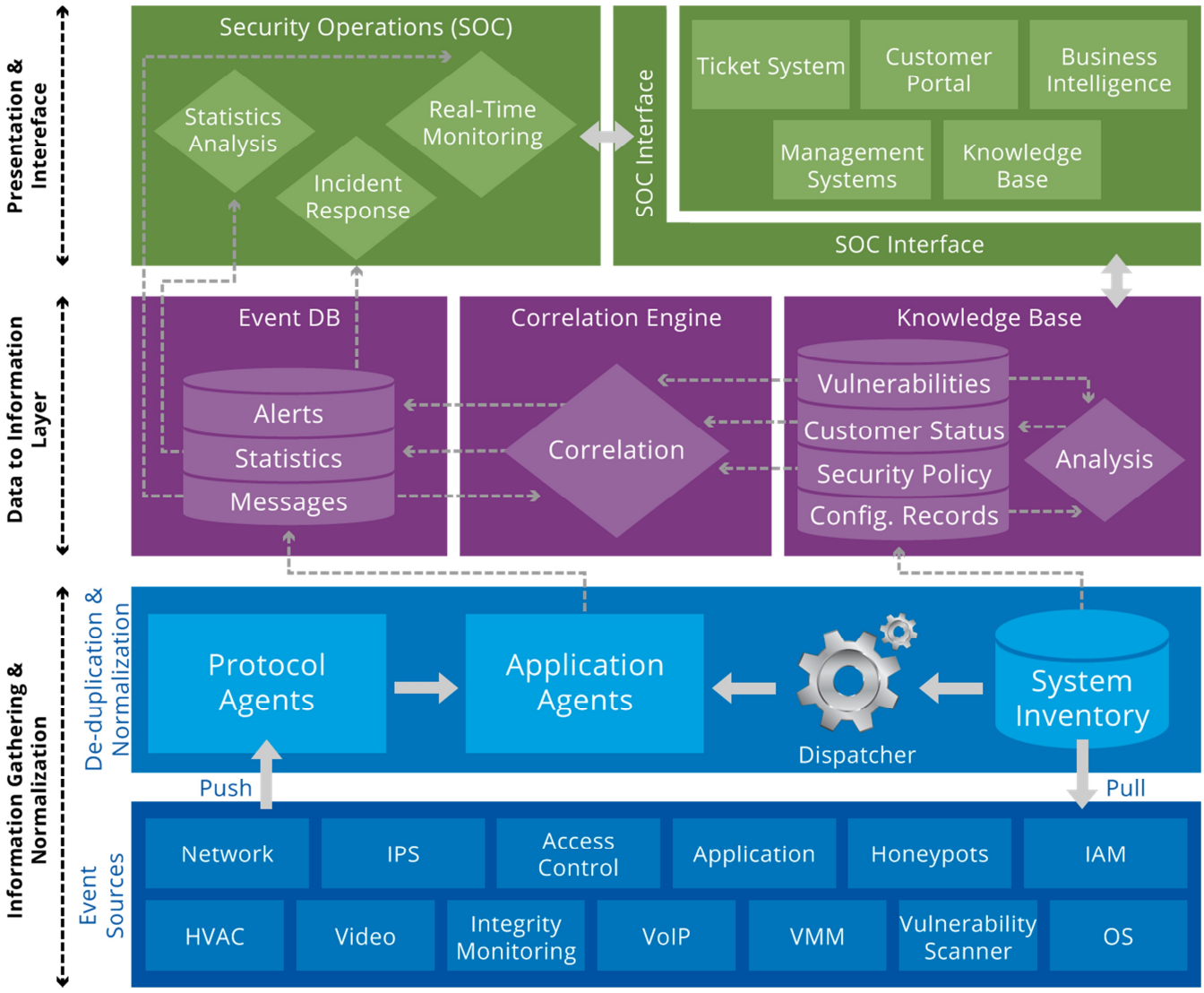


*Figure 3: SIEM Reference Architecture*

## 4.1.2 SIEM Inputs

The SIEM system receives input from other security solutions as sources; it then provides output to response processes. SIEM is the core component to aggregate, normalize and monitor security events across a broad range of network, security, host, database, and application components. It also provides security information normalization, context, correlation and analytics.

In some SIEM solutions, Log Management is a built-in or add-on component designed to work in conjunction with an existing log management solution or to replace it. For some log management solutions, SIEM is the add-on that can be acquired. SIEM takes input from network, host, database, application logs and other security tools such as Vulnerability Management systems, firewalls, anti-malware systems, Data Loss Prevention systems

(DLP), honey-pot and honey-net systems, and Intrusion Detection/Protection Systems (IDS/IPS). It may also gather data from network devices, servers such as Domain Name Servers (DNS), WEB servers, Active Directory (AD) servers, database servers, and other key computing resources so that anomalies in network devices (switches, routers, Wireless Access Points [WAPs], etc.) and system performances can be detected. Less traditional sources of data can include Identity and Access Management (IAM) Systems, facility HVAC systems, occupancy sensors or the lighting systems they control, Closed Circuit Television (CCTV) systems, fire control systems, power management systems, and any other system that can provide pertinent data that helps define a security event in the enterprise. A SIEM system can take almost any input that can be digitized and, through a well written rule-set, will create an output.

### 4.1.3 SIEM Outputs

The output generated by the SIEM can be consumed by a number of third-party systems including incident response systems, auditing systems, maintenance systems, helpdesk ticketing systems, and other phases in the defense lifecycle. One of these systems, the Enterprise Security Intelligence (ESI) is a core analytics component that extends the capabilities of a solid SIEM implementation. Security intelligence is an explicit deliverable and aim at increased accuracy and breadth of security detection and protection, as well as optimal security management. Technically, ESI could be achieved by custom analysis, scripting or coding as an extension of SIEM with strategic objectives for enterprises' IT security and risk management.

Other deliverables include system compliance reporting to monitor real-time compliance with pertinent rules and regulations. These could be standardized reports created regularly or could include *ad hoc* reports in response to specific regulatory or leadership queries. Network and system performance data is often a security domain (availability) that many architects ignore. Since all the network and Server systems feed their logs into the SIEM, it stands to reason that the network and server management functions may be interested in the infrastructure reports it is capable of generating in order to ensure the continued availability of the enterprise network. For the network architecture and security architecture teams, the historical performance data available from the SIEM logs provide important insight into where future problem areas may arise and allow them to act proactively to ensure continued availability and integrity. The HR department may also leverage the SIEM system to requested reports on employee activities and potential malfeasance. Active investigations can be further assisted and automated using the SIEM to track an employee's activities on the net in real-time.

When implementing SIEM as SecaaS SIEM only (as opposed to a hybrid system), it is likely for the provider to install a log aggregator and collector within the local network of the customer. The log aggregator abilities should match customer requirements and should be suitably positioned within the network to ensure protection from internal and external attacks. Here is a list of common requirement by customers to review with your SecaaS SIEM offering:

- The log aggregator should support all protocols used for logging within the enterprise.
- The log aggregator should have the ability to store logs for a specified amount of time if provider server is unavailable or somehow disconnected.

- Logs sent from aggregator to SecaaS SIEM provider should be encrypted, either by VPN, encrypting the logs at source, or using trunk encryption devices. Note that SSL VPNs typically add a 30% overhead to the data stream, which must be considered when capacity planning.
- Some log aggregator can mask or filter out log items that contain confidential information. Internal compression of logs before sending SIEM provider can help handle risks such as network latency.

### 4.1.4 Operations

The SIEM system architecture should also reflect the security operation edicts set forth by the enterprise. This reflects how the alerts generated are monitored and who is monitoring them. If the alerts are monitored locally, the infrastructure would be different that if monitored at the vendor. The subsequent response pattern should also be addressed to include how communications will occur between the monitoring center and the IT staff. If the monitoring is accomplished by the SIEM vendor, then a DOS attack would preclude the IT staff receiving any email or SMS messaging alerting them. Conversely, if all alarms are monitored locally, a breach and subsequent DOS attack in the cloud could take hours to receive eliminating the ability of the network and security personnel to respond.

The response to alerts will dictate further security and architectural considerations depending on how incident response is directed. If the SecaaS vendor is accountable for the response to an alert, considerations must be given to how the vendor gains access to respond to the alert and how the enterprise IT staff and management is kept appraised of their actions.

## 4.2 Guidance and Implementation Steps

While the legal and architectural details of a SIEM system implementation are crucial in ensuring the implementation of a successful SIEM system operation occurs, it is the operational analysis and the rules that guarantee that serves its intended purpose.

### 4.2.1 The Key Considerations of SIEM

An effective enterprise security management system must encompass the key considerations of SIEM systems:

1. **Comprehensive Enterprise Coverage** – All production layers (networks, hosts, applications, databases, identities) and environments (on-premise and cloud) must be considered as suspects of advanced attacks and covered by SIEM system, even if they appear to be "healthy."
2. **Information Interaction and Correlation** – The SIEM system must have security data input sources from events and logs of all network devices, hosts, databases, applications and identity directories in order to create a full threat knowledge base for the enterprise. It is vital to intelligently correlate information to derive meaningful information from a flood of data. Any systems not connected to the SIEM system is therefore a non-player and its information cannot be used to detect and generate alerts, and any attacks on them are virtually undetectable.
3. **Technology Interaction and Correlation** – The SIEM system must be integrated with other security technologies, such as IDS/IPS, Firewall, DLP, IAM, Vulnerability Management, firewalls, and Anti-

Malware systems. Those technologies are correlation sources in order to lower false positive rates, increase accuracy and breadth of security detection.

4. **Business Interaction and Correlation** – The SIEM system must be aware of business context. Advanced attacks are usually targeted with a great deal of business information. When interaction and correlation is extended with business information, ISRM will be capable of thinking as the enemy, predict an attacker's priorities, reduce the noise, and derive more meaningful intelligence.
5. **Cross-Boundary Intelligence for Better Decision Making** – Security activities and the intelligence that results from SIEM output must not be in isolation. Organizational boundaries must be crossed by the SIEM system to achieve enterprise security intelligence and support decisions for protection, response, and recovery.
6. **Visualized Output for Dynamic and Real-time Defense** – The output of SIEM system must be visualized to help drive preventive and corrective controls, to stop advanced attacks or block data exfiltration attempts. Only easily consumable output can drastically reduce response time, minimize damage, and all quick response to investigate and determine root cause of security issues and breaches.

## 4.2.2 Logging Configurations

Operational rules require specific log data from all network systems being monitored. For example, merely by pointing the logs of a domain controller to the SIEM system does not guarantee that the logs related to employee log-in and log-off can be obtained. Unless the audit policy setting on a domain controller is properly configured, that data will not be sent out to the logging facility or SIEM system. Windows domain controllers offer 16 different options just for DNS logging. Similar logging criteria exist for nearly all other systems tied to the SIEM system. Thus, it is incumbent upon the security analysts operating the SIEM system to ensure that they receive the feeds necessary to make the proper analysis and alerts required by the business. In order to do this, the analysts should determine:

- Which elements of the data provide the necessary context
- Which exact fields are relevant
- If the data frequency supports the proposed solution
- If the data resides in a centralized, easily accessed location
- If the data is raw or has it already been aggregated, normalized or filtered in a way that would adversely affect the proposed solution

Each of these factors should be analyzed to ensure that they support the needs of any proposed rules. Logging configurations should be documented with documentation as to what each data feed is needed for. Finally, these data feeds should not be considered final in any way. As the needs of the business change, as vulnerabilities and operations change, the rules will require different data feeds to accomplish the business objectives of the SIEM system.

## 4.2.3 Building Rule Scenarios

One significant stumbling block that most security teams have is selecting or building the rules provided by the vendor. Some are tempted to enable all the rules or a significant portion of rules provided thinking that it will

help secure the enterprise. It will most likely bury the security staff in false positive alerts and may more significantly allow situations that should have alerted go unnoticed (false negative). The simplest way to prevent chaos and to start building the rule sets that supports the business drivers is to build individual scenarios to describe violations that should be detected and responded to and the business, legal or regulatory justification. The scenarios should include the situation and subsequent response, and are best when they contain active verbs. The following are a set of simple scenarios:

## Scenario 1 – Enterprise Correlation and Sharing

Ed is a Security Analyst on the Security Investigation team. He used a different SIEM system from the one used by IT and other organizations. Fortunately, all SIEM systems use a common information sharing format. Ed configured his SIEM as the hub to get aggregated information from all SIEM systems, both on-premise and in the cloud. He was able to correlate data companywide, share information with other IT organizations, and view the security posture of the entire enterprise from a single pane of glass.

## Scenario 2 – Incident Response Enablement

Georgia is a Security Analyst on the IT Operations Response team. Prior to the SIEM deployment, she spent most of her time collecting vulnerability information and triaging an event. Only a small percentage of her time was spent dealing with real incidents and working with the forensic team. After the SIEM deployment, her vulnerability information workload was taken over by SIEM in an automated vulnerability information feed. She could also quickly assess events during the triage time. The best part was that most events were correlated and classified as noise by SIEM automatically. When a real attack incident happened, Georgia was able to quickly contain the compromised system and work with other teams to help with the recovery phase.

## Scenario 3 – Malware Protection

Matt was an Anti-Malware architect in Security Operations team. Recently he felt that endpoint anti-malware was not able to cover 100% of his needs. Some modern malware didn't have signatures or patterns that the anti-malware could detect or recognize. The enterprise malware reporting was provided by the anti-malware server which is unable to correlate malware events with other security events. Correlation rules were configured to link malware data with vulnerability data and asset data. The rule used vulnerability data to qualify systems that had a chance for infection. The asset data helped link infected systems to it owners, business roles and other asset parameters.

Finally, alert rules were set up and for infected systems, alerts were sent to owners and the operations team if the malware failed to be cleaned. Other alerts were also trigged for repeated failed signature updates or internal systems attempting to connect to systems/websites on the malware blacklist.

## Scenario 4 – Tracking User Actions across Disparate Systems

Kim was a security analyst on the Security Investigation team. One day, her manager called her into an emergency meeting with people from the Security, Legal, and HR teams. She learned an anti-company article was published in the Wall Street Journal. An anonymous author criticized her company for outsourcing jobs abroad that hurt employment in the United States. A lot of detailed facts, such as contracts with India and Chinese outsourcing companies, were shown as examples. This article trigged several demonstrations and press attacks against the company. The team concluded that the author was an insider and asked Kim to help.

Kim then created and ran a custom SIEM user action report and specified a few disparate system logs including the enterprise resource planning (ERP) system, contract management system, and the web servers' logs used by outsourcing projects. Based on user access activities, the report generated a list of suspicious users. After further investigation of related activities, one of users was identified as the top suspect because they tried to access related systems and servers more than others in this period of time. Additionally, they downloaded related contract files that matched the content in the Wall Street Journal article.

Based on information from SIEM, the insider got caught, unable to deny their activities, and was finally terminated based company policy.

## Scenario 5 – Server User Activity Monitoring

Sam was a new hire in the Security operations team. One day, he configured the newly deployed SIEM to collect login success/failure events from all servers in both on-premise and cloud environments. In the next few days, he averaged a daily baseline of failed logins in SIEM. Based on his analysis, he configured two additional rules on the SIEM.

- A correlation rule: the daily logon failure is ##% more than the baseline.
- An alerting rule: x number of login failures on any server in y number of minutes followed by successful login within z number of minutes to the same server

Finally, he tuned the numbers through testing, so SIEM would generate a reliable login anomaly report from the correlation rule and trigger alerts from the alerting rule without producing "false positives."

After the rules were established, Sam's team was able to see the server login anomaly trends in the dashboard, add this data into the security health index for the CIOs scorecard, and receive alerts when a particular server is under a brute force password attack.

## Scenario 7 – Web Server Attack Detection

Wendy was a Security Engineer who has spent a lot of time performing line of business web application security code reviews, static code scans, and pen tests. However, she still could not guarantee web applications were 100% security bug free. She knew that most external attackers were exploiting website vulnerabilities and this had led to a vast majority of security breaches.

Wendy was happy that the SIEM team worked with her and her internal customers to configure SIEM to detect attacks against Web Servers and Web Applications. They decide to feed Windows event logs, Web server logs and Web application logs into the SIEM.

Finally, she was able to use a rich set of reporting from the dashboard to monitor the websites:

- Report: Trends of errors by type over time
- Report: Injection attacks and pattern (*.exe or suspicious strings from visiting browsers)
- Report: Web server– Top 10 page not found (error 404)
- Report: Web server – Top 10 Script Errors (error 501)
- Report: Web server – Top 10 Authentication Failure (error 401)

## 4.2.4 Rule Documentation

One of the most important items for a security team relying on rules is to carefully document all relevant information pertaining to the rule. The documentation should, at a minimum, include the following information

- **Purpose:** What is the purpose behind the rule? What business need or vulnerability does it address?
- **Author**: Who do we contact if there is a problem?
- **Action**: Action(s) and/or Output(s) required from the system when the rule is triggered.
- **Actor**: Relative to a *(PERSON/TEAM)* who do we notify when the rule is triggered? If a significant corporate decision needs to be made as a response to the alert, the actor should be empowered to make the decision by the senior leadership.
- **Event**: Specific scenario(s) to be evaluated. What action should we take when the rule is triggered? What do we go looking for and where?
- **Context**: Relevant environmental conditions. How does our knowledge of this environment affect how we can refine the analysis and output? Some examples of context that should be considered are:
    - Organizational Structure
    - Business Units
    - Application and/or Data Categorizations
    - Network Segmentation, System Configurations
    - Users
    - “Hot Lists”
    - Vulnerability Data
    - Data/System/User Criticality
    - other environment specific information
- **Timing**: Within, before, at, during, after. Receiving the exact time from your devices can be tricky when working with a SecaaS SIEM because the provider can monitor many devices from different time zone. Tests are required on each device to make sure the right offset is applied and that the time stamps are clearly understood.
- **Logic:** Boolean Logic Statements (T/F) using AND, OR, IF, THEN, NOT as conditions.

- **Response:** These are the active statements that indicate what the response should be by all actors. "The system shall," "Security staff must page/notify Compliance." We have to" *(DO SOMETHING)*.

Without this information, performing an analysis or attempting to understand an alert can become a difficult and time consuming task. The documentation enables security analysts to quickly look-up pertinent information to the alert and determines what actions to take. It also enables much quicker response times for newer personnel assigned to the Network Operations Center (NOC), Network Operations Security Center (NOSC), or Security Operations Center (SOC). It also ensures that any requirements to notify compliance officers, take actions, or gather data for breach solution systems is completed immediately. This is particularly important for healthcare, financial and banking industries where breach notification requirements are legally required to be prompt.

### 4.2.4.1 Correlation Rules

The most effective rules for correlation in a SIEM system rely on rules designed to address specific behaviors on compartmentalized segments of the network. While accessing financial management systems may be normal for systems in the financial department, accessing records in Engineering or Research and Development is not. Thus, the rule set needs a baseline pattern and behavior based on the business activities and systems they support.

SIEM tools also require a lot of tuning. Rules have to be built with great care and attention to details in order to work as intended. Well written rule sets will minimize false negatives and false positives enabling the security staff to focus on meaningful alerts. The continued tuning of the rules by the security staff will ensure that progress is made in these areas and that rules are updated to reflect changes in business practices, network behaviors, and systems. By carefully documenting the logic and assumptions in each of the rules, when corrections need to be made it can usually be pinpointed to a specific assumption or data point that needs to be corrected. Rules must be carefully tailored and tuned to address the specific event that they are attempting to detect.

Different SIEM systems leverage different rule constructions as appropriate to address specific applications and events. These range from the simplest rules such as audit rules, to the most intricate rules, the inference-based rules. As always, complexity is the enemy of security so rules should be developed using the simplest algorithms possible that will accomplish the task. Every rule could be written as an inference-based rule but it would consume excessive resources and be more likely to fail when needed most.

For some SecaaS SIEM vendors, all rules are predefined and an enterprise can choose to turn on or off any given rule based on their business drivers. While this may be effective for some situations, it does not allow for the tailoring or development of rule sets to address typical network behaviors and therefore may be of limited value to many enterprises. Some vendors provide standard rule sets and then can create customized rules for individual customers to support specific business requirements, for a fee. The advantage is that an enterprise could simply express to the vendor how they want the rule to work without having to have their own analysts know how to create or modify correlation rules. Then there are vendors who not only provide standard rules and rule writing for a fee, but also enable the enterprise analysts to tailor specific rules or author new rules to

 

address specific business needs or vulnerabilities within the enterprise. While this is the most desirable for mid and large enterprises due to the flexibility it provides, it is often the more expensive option.

### 4.2.4.2 Audit-Type Rules

The Audit rules are the simplest of the rules as they are looking for a condition to exist or not. An example of an audit rule would be when there is a change in privileges for an account, when a password expires, or when there is a log-in failure for an administrator. The rule works as follows:

*Event* **A** = *Alert* **B**

It simply reports that an event has occurred. Due to its simplicity, very little processing overhead is spent on these so these tend to be the most desirable of the rules but because of its simplicity, it has a very limited use.

### 4.2.4.3 Signature-Based Rules

Most anti-malware systems rely on signature-based rules to detect infections of viruses, worms, and attack tools. The signature is a list of patterns that when they occur, an alert is generated. An example of how the rule could work would be as follows:

*Events* (**A** OR **B** AND [**C** NOT **D**]) **=** *Alert* **F**

These patterns are often used to detect specific malware or attack patterns in the enterprise and react when a pattern is matched. The logic is typically very simple and can generally be expressed in simple Boolean terms.

### 4.2.4.4 Heuristics-Based Rules

These rules leverage a collection of rules and patterns based on prior structures, routine and behaviors. Where signatures detect events based on strict patterns, heuristics look at patterns and behaviors, and evaluate them by assigning each a risk factor. If the risk factor count exceeds a certain threshold, then the alert is triggered. These types of rules are commonly used to identify root-kits because experience has shown that root-kits can hide themselves from host-based detection systems but give indications of their presence on the network by the patterns they exhibit. It is often thought of as a means by which rules look for similarities to known malware behavior. This is also what many systems refer to as zero-day-exploit detection since the heuristic engine does not need to know the exact pattern, just the similarities between it and known malware patterns.

*Compare Patterns* **A** AND **B** AND ….**F** *with Pattern* **X**.
IF *similarity count exceeds* **Y** *then Alert* **Z**.

### 4.2.4.5 Inference-Based Rules

Rule sets that leverage Bayesian inference logic have become more popular as the accuracy and understanding of Bayesian predictions grows. This type of logic has now been used for several years to help predict and combat spam. Using known patterns and changes in those patterns, a Bayesian inference-based rule attempt to predict an event before it occurs. It relies on comparing a hypothesis that a given event may occur given a series of prior events that may have shared some similarities. A Bayesian filter then takes a population of hypothesis,

compares it to the statistical similarities of the evidence presented, and estimates the probability that an event has or is occurring. Like with the Heuristic-based rules, if the probability exceeds a statistical level set by the organization, it triggers the alert.

This is particularly useful when attempting to detect criminal behavior (insider trading, IP theft, etc.), breaches, both internal and external, and other nefarious behavior. It is often used for behavioral anomaly detection. Certain behaviors on a network are extremely consistent over time and if the behavioral patterns of users and systems are recorded by the system, when the behaviors change more than a specified deviation set by the analysts, an alert is triggered. While some behavioral patterns can be detected by heuristics, the more efficient rules rely on Bayesian inference to predict whether a deviation in the pattern is potentially nefarious or not. It is the most effective tool against zero-day attacks.

### 4.2.5 Rule Responses

Having developed the rules, it is also important to examine what reactions should take place as a result of a rule trigger. This should not be based on the rule type but tied back to the business drivers to help determine the severity of an alert. Once the severity is understood, the response must also be examined to help determine the notification means. The documentation discussed in section 4.3 will indicate who should be notified. Now depending on the severity of the alert, one also has to determine by what means the notification goes out. For high priority alerts, the most likely notification method will be a page, an SMS message, or a text message to a cell phone. For lower severity alerts, notification could be done via email or simply a data point that appears on a report. The following is an example of how an alert chart would look:

| SOURCE | NAME | ALERT CONDITION / CORRELATION | SEVERITY | ALERT TYPE |
|---|---|---|---|---|
| Active directory | Changes made to GPO | Change made to financial department OU | LOW | MAIL |
| Active directory | User created | Created in off hours | MEDIUM | SMS |
| Check Point | Failed login to CP console | Over 3 times in one hour | HIGH | SMS |
| Firewall + VPN device | Port scan and auth attempt | Detected port scan followed by authentication attempt from same IP in one hour | MEDIUM | MAIL |
| SAP R3 | User access transaction SU01 | Source terminal is not IT department | MEDIUM | MAIL |
| Active directory | No check-in for 30 days | A laptop computer has not checked in to the network for 30 or more days | LOW | REPORT ONLY |
| Active directory | No check-in for 30 days | A Web server has not checked in to the network for 15 or more minutes | HIGH | SMS |

This is only a short list of possible alerts and responses. A full list should be developed, maintained, and updated regularly by the security staff.

## 4.2.6 Operational Needs

When examining the operational needs of the response system, it is important to verify that all communications paths are redundant. VOIP phones should have a POTS line or cellular line as a back-up and network connections for the SIEM connections to the SIEM vendor should have multiple independent paths identified. Other operational features that should be examined by the security staff include the placement of a graphical event overview (a map of the network and the issues) which enhances the abilities of analysts to respond to breaches and infections by providing a quick look to determine where problems lie and how they are progressing or spreading. Log Drill-down capabilities so that records can be examined by IP address (internal and/or external), Machine ID, User name, Protocol.

## 4.2.7 Quality Assurance

Quality Assurance is an ongoing activity. It ensures that rules can be properly tested in an operational environment without the risks associated with testing them on the production system. A proper lab setup should mirror the production system in every way to ensure the outcomes on the production network systems are predictable. Using canned or irrelevant data/systems renders the tests meaningless. Knowing how the system is going to respond before implementation into production saves time, effort and a lot of headaches.

QA should include simulating all rules agreed between customer and provider to make sure they are triggered correctly, tests including disconnecting the line to the provider to make sure logs are not lost, and the testing of response scenarios on a quarterly or semi-annual basis.

Finally, if a rule fails to function, the first place to look is to ensure that the system generating the log data needed for correlation must be supplying it. The number one reason for support calls for SIEM rules are remedied by turning on the log data at the source so the SIEM facility can see it.

# 5.0 References and Useful Links

## 5.1 References

Kavanaugh, K. and Nicolett, M. (2012, May 24). *Magic Quadrant for Security Information and Event Management*. Stamford CT; Gartner Inc.

Kurtz, G., McClure, S., and Scambray, J. (2012). *Hacking Exposed 7: Network Security Secrets & Solutions*. 7th ed. New York; McGraw-Hill.

Laundrup, J. (2008, July). *Detecting Insider Trading using Automated Correlation*. Adelphi MD; University of Maryland.

Laundrup, J. (2009, June). *Data Security Breaches: An Unstoppable Epidemic?* CISO Lecture Series. The State of California Office of Information Security. Sacramento CA.

Laundrup, J. (2011). *Implementing SIEM in the Enterprise: A Plan for Success*. San Carlos, CA; Emagined Security Inc.

Laundrup, J. and Schultz, E. (2011, March 28-29). *Cloud Computing Security and Auditing*. Seattle WA; ISACA-Puget Sound.

Net Forensics (2008). *10 Mistakes to Avoid in Evaluating Security Information Management Solutions*. Edison, NJ; Net Forensics Inc.

Pack, D. (2011, April 12*). Using Correlation Rules To Perform Decentralized Threat Detection.* The DiaLog powered by LogRhythm. Retrieved from http://blog.logrhythm.com/security/using-correlation-rules-to-perform-decentralized-threat-detection/

Schultz, E. (2010). *Cloud Computing Security: A Look into the Future*. San Carlos, CA; Emagined Security Inc.

Schultz, E., (2009, June 17). *The In's and Out's of SIEM Technology*. IX National Computer and Information Security Conference. Bogota Colombia.

## 5.2 Useful Links

The following is a list of places where additional information can be gathered about SIEM implementations:

Book review, but provides some SIEM details and links to a potentially useful SIEM book for those who want to read further: https://365.rsaconference.com/blogs/securityreading/2011/02/24/security-information-and-event-management-siem-implementation

Details some SIEM challenges: http://www.darkreading.com/security-monitoring/167901086/security/security-management/227500819/index.html

 

SIEM dos and don'ts: http://www.csoonline.com/article/509553/siem-security-info-and-event-management-dos-and-don-ts

Cloud creates SIEM blind spot: http://www.darkreading.com/security-monitoring/167901086/security/security-management/228000206/cloud-creates-siem-blind-spot.html

Cloud vs. SIEM challenges: http://securecloudreview.com/2010/08/service-provider-of-tomorrow-part-9-as-the-cloud-thrives-siem-will-suffer/