Log Management and SIEM Evaluation Checklist

Authors:
Frank Bijkersma (frankbijkersma@gmail.com)
Vinod Shankar (e.vinodshankar@gmail.com)

Published on www.infosecnirvana.com, www.frankbijkersma.com
Date: May 2014
Version: 2.0
1. Introduction:

Security Information and Event Management (SIEM) is an industry that is filled to the brim with solutions to “manage your logs”, “correlate logging” and “keep your company in compliance”. But often the multitude of choice and diversification does not translate to a clear single solution that is fit for your companies needs.

This guide assumes you are already knowledgeable about what a SIEM is a, but for the uninitiated, we have given a brief introduction of what SIEM is below.

What is a SIEM?
SIEM as a product is an odd one out, touching every appliance (if implemented correctly of course) in the (business critical) IT-infrastructure but not directly supporting any critical business processes like your Windows Domain, SAN or Application servers do. The only exception here would be if you are an Managed Security Service Provider (MSSP) offering a SaaS SIEM service.

A SIEM is a product that is used by business users such as an Chief Information Security Officer (ISO), internal and external auditors and if you’re company is big enough personnel from the Security Operation Center (SOC).

Before selecting a SIEM vendor you need to make sure that the product meets certain selection requirements. SIEM is mainly a direct end user product that provides an ability to perform Real time Security monitoring. Security has become a key functional unit in an IT Infrastructure and Organizations need to have a solid understanding of the various parameters in selecting SIEM products.

This guide is meant to be a comprehensive list of pointers which you should consider in your selection criteria when you are selecting a SIEM solution (and if you actually need one). After identifying your actual needs you will find 7 area’s on which the software (including the company and services offered) as well as the implementation and use of the software in your company can be scored. The pointers for each area are as broad as possible but by no means exhaustive. The pointers don’t provide a weighing or value as these are different for each company. Lastly the pointers are generic by design to allow for a vendor neutral approach.

The best way to use this guide is to read it through one or two times, highlight point of interest for your company to get an early idea of what you may preliminary select on in the market and then start at chapter 2 with your stakeholders and define your requirements.
2. Setting your scope and requirements

Before starting a SIEM selection it is fundamental to know why you are in the market for one as it heavily influences the weight you have to give to certain features. These are the most common reasons to have a SIEM;

1. Security Incident Detection & Response
With Security Incident Detection and Response you are analyzing your company's environment logging in (near) real-time and reacting accordingly to threats and breaches. Often this takes form in a Security Operation Center (SOC), though smaller companies often have a Network Operation Center (NOC) that doubles as a SOC. Implementations often include hundreds of servers, firewalls and other devices, dozens upon dozens of rules and heavy use of correlation between all these.

2. Compliance Monitoring & Reporting
Compliance mainly focuses on showing the auditors and regulatory bodies that you indeed are complying with their (or your own) rules for configurations of systems and network devices. You will not be monitoring in (near) real time and mostly will only be reminded of the product when the weekly or monthly report comes in (or the auditors visit is just weeks away).

3. Operational Requirements like Troubleshooting and Log Management
With this reason we are mostly looking at the people that are on an operational level, though sometimes it is used as a rudimentary form of Monitoring and Reporting. Often there is no need to actively do much with the logging, unless you are troubleshooting, doing a monthly check on some predefined points of interest (such as root usage), or want to keep it around just in case you need it.

This is not to say you only buy a SIEM solution only for any of these three reasons. But often a company that only needs Compliance Monitoring and Reporting can do with a cheaper and less feature rich software than a company that needs Security Incident Detection & Response. Secondly you will need to establish the types and number of the devices you want to attach to your SIEM, often SIEM is only affordable (and needed) for companies that are midrange to enterprise size.

Products like Splunk, GFI Event Manager, LogLogic, LogRhythm, Syslog-ng Store box, Win Syslog, Kiwi Syslog etc can be a quick a dirty way to collect, store, process and report on the logs. Which is likely to be more than adequate to address compliance monitoring and reporting as well as operational requirements like Troubleshooting and Log Management. These products also support Log Filtering and Log Search. These can most of the times satisfy the needs of Operations teams for troubleshooting, for Log Reporting, basic compliance metrics etc.

However, the moment you step into the space of Incident Detection and Response, the need to perform Log Correlation, Log Analysis and Workflow comes into play. This is where the SIEM players come into the picture. The SIEM players in the market are HP ArcSight, IBM QRadar, Splunk ESM, McAfee Nitro View, RSA Security Analytics, Trustwave, Alienvault etc and these provide Incident detection using their proprietary Correlation engines called the Enterprise Security Management .

The 5 key things to consider in buying and implementing a SIEM solution are:

1. **Log Collection capabilities** – Using an Agent based approach or Agentless approach, out-of-the-box log collection support for 3rd party commercial IT products
2. **Parsing & Normalization** – Collected logs will be parsed and normalized to a standard format for
easy storage, analysis & reporting

3. **Correlation** between Events of different type thereby helping in threat identification. Example: If Event A is followed or matched by Event B, take an action.

4. **Real-time Notification and Alerting** – real-time alert on Security threats in the IT environment based on analysis of collected logs.

5. **Security Incident Detection & Response Workflow** – Operations Workflow for handling detected security incidents and threats.

3. **Company & Product:**

A SIEM product (or any other software product for that matter) is as good as the company that develops it. This is a key consideration because a company that is stable and has a long term road map focusses better on product development and building expertise. Hence, evaluating the company also becomes important when buying the product. The following are a list of criteria you can use in your selection:

**General information**
- The Industry Focus, Market presence and Years of experience in the field of the Vendor.
- Financial Performance - Subjective Measurements over the past years will give you an indication if the company will stay around for the intended lifetime of the product.
- Know the Executive Leadership of the Company. Is the leadership team strong? Is it Trustworthy?

**Focus and vision**
- How strong is their product road map?
- Dollars spent on R&D for new products versus Development on incremental growth of core product.
- Is the vision of the product group forward thinking? Are they innovative?

**Third party ecosystem / partner programs**
- Does the company (or the specific product) allow for 3rd party developers?
- Does the company actively support and empower 3rd party developers, for example by publishing API documentation, SDK, debugging software, online marketplaces, dedicated forums etc.
- Does the company have a partner program and allow 3rd party consultants?

**Publishing**
- Company engagement in industry conferences, congresses etc.
- Company publishing presentations, white papers, research papers, documentation
- Company publishing (free) tooling

**Industry opinion**
- Marketplace opinions and reviews about the product and the company as a whole.
- Do they have customer references for both the product as well as the company?
- Analyst Reports for the last few years - Gartner, Forrester etcetera.
- Do they have a track record of successful product launches, revisions, development etcetera.
- Is there expertise across the vendors partners (VAR, MSSP, Consulting Organizations) to support both basic and advanced consulting needs? How mature is the partnership or alliance relationship?

**Security and Trust**
- Has the company had any security incidents or concerns about its integrity?
- Is the software known to have had (severe) security vulnerabilities in the past?
- Has the company responded to and resolved previous incidents correctly and professionally? (if
4. Licensing, Training and Support

Though we are still far from buying a SIEM product, it is best to address the key consideration in any company early on; the total costs of ownership (TCO) for the SIEM system. Costs will be comprised mostly of the licensing costs (one time or spread over multiple years), hardware costs, Support (support contract) and training and certification of your own personnel. Other costs will need to be addressed separately.

Licensing
- Are licenses limited to a certain bandwidth, active users, EPS?
- Are licenses bound by a certain timeframe (1 year) or perpetual?
- Are licenses flexible in upgrades; e.g. upgrade EPS limits, active users.

Hardware
- Limited to hardware of the SIEM vendor, or free to use your own hardware?
- Does it have a Range of hardware requirements that can help map my equipment standards? or does it only have high end hardware as standard requirements?

Support
- How is the Company’s product support and services group?
- Is it a dedicated team in house or is it outsourced?
- What are the product support professional services options available?
- How focused is the management team in providing Support services?
- Is support available globally? is it 24/7? Are there support levels?
- Support methods (Phone, e-mail, forums, tickets, chat etcetera).
- Is support available in your native language?

Certifications & Training:
- Training options for the product - Classroom? Online? Mixed?
- Certification options for personnel
- Continuous training options available for new product releases, feature releases etcetera?
- Are there many Certified people available in the job market that can work with this product? This is especially important when building a SOC or using a SIEM product in general.

5. Architecture:

One of the key components of a product is its architecture maturity. The product should be capable of catering to IT Infrastructure needs that vary from industry to industry, from enterprise to enterprise. Some of the key questions related to Architecture are listed below:

Hardware
- Are you limited to hardware (appliances) of the Log Management or SIEM vendor, or are you free to use your own hardware?
- Does it have a range of hardware requirements that can help map equipment standards? or does it only have high end hardware as standard requirements?

Flexibility
How flexible is the product deployment architecture? Can it be run as an Appliance, a Software standalone, a virtual appliance/machine or a Saas?

Can the architecture be deployed in a way where individual data storage capability is available per business unit/location?

Does the architecture allow for full data replication for HA purposes? Is HA a built-in function or additional equipment is required?

Does the architecture allow for interoperability with Network Management devices, System Management devices etcetera.

Does the architecture support scalability? Is it modular enough to expand based on growth needs, storage needs and performance needs?

### Security

- Does the product support granular Role based Access control for the underlying hardware & application software?
- Does it meet the organization’s policy and standards compliance requirements
- Does the product have a secure data transmission between Event Collection, Event Storage and Event Correlation layers? Does it use encryption? If so, how strong?

### 6. Installation, Configuration & Maintenance:

When installing and configuring the software for the initial setup and future refinements and general management:

#### Pre-Installation

- Are changes needed to your current setup - e.g. changes in policies, ports, firewalls
- What are the supported platforms - e.g. Windows Server 2012, Red Hat Enterprise 6.5
- Additional dependencies - .Net Framework, Java Runtime etc.

#### Initial Installation

- Can the Installation and Initial Configuration be handled by technical staff (w/o training)?
- Ease of set-up, Maturity of Product Documentation and Support to facilitate this effort?
- How long will installation and configuration take? Does the vendor give an indication

#### Post Installation

- Ease of post install maintenance, patching, routine tuning?
- Installation of software updates, content updates, Operating System updates

#### Storage

- Does the product allow storage of data locally, remotely in a SAN or NAS?
- Is the data storage capable of compression? If so what is the rate of compression?
- Is the storage architecture dependent on standard database or does it use proprietary architecture? If proprietary, does it have all the capabilities to meet storage security requirements?
- Is Data Archival flexible? If so, is it built-in? What options does the product have?

### 7. Day to Day operations

One of the key criterion to select a SIEM is “How easy is it to Operate the product in a dynamic
Operational environment?” Some of the pointers that can help you make that decision is as follows:

**Interface (Ease of usage)**

- Is the interface a standalone client console or a web console?
- Is the interface easy to navigate and use, or highly user centric and technical?
- How is the performance of the User Interface?
- Does the interface need additional software installed?
- Is the interface portable among devices (Computer, Tablet, Phone)
- Does the interface allow easy access to actionable data? Does the interface organization require a steep learning curve? Can the analyst drive deeper analysis or via tools with a single action (right click and select)?

**Product performance**

- Performance when searching for various data elements (IP addresses, usernames, event types, etcetera)
- Performance when generating reports, query results, data extracts?
- Performance when high volume of events or a sudden surge of events occurs either unexpectedly or as a part of a Targeted attack?

**Segregation of duties**

- Can access to data in the system be restricted according to access rights (i.e. business units can see “only their data”)?
- Can the console present just the events a particular analyst is assigned to handle?
- Can granular role based access matrix be defined?

**Handling of Assets**

- Will the product function to support the needs of the Tier based SOC Analysts, Incident Handlers, Responders?
- Is the data presented in a manner that makes sense to the analyst?
- Can analyst understand correlation actions?
- Can analyst easily change correlation actions?
- Could the product act as an incident management tool, accepting case notes, and related information on an incident?
- Is the software designed to track user input to understand how users interact with the system? Objective measures of feature use (misuse)? How is this information mined? Are there any Privilege user management content to audit and track privilege access?
- How does the product or solution facilitate asset tracking?
- Interface to 3rd party applications (ticketing/workflow application, existing business logging solutions etcetera.)

**8. Rules, Notification, Reporting and Analyzing**

Every operations team needs a workflow. Notifications, Reporting and Incident Investigation and Analysis form a part of that workflow. A SIEM platform should provide the flexibility to an analyst to have an optimal workflow pattern.

**Rules**

- Does the product support the most difficult use-cases for correlation? (Multi Vendor, Multi-Event, Custom Application and Custom field correlation)
- Can the system support “live”, “custom”, or “dynamic” threat feeds for live correlation and alerting? Threat Intelligence Feeds such as IP’s, Subnets, Domain, Files, Patterns, etcetera.
Does the concept of a “Hot-list” or comparison list exist? Automated Hot-list Trigger. A Hot-list can be a watch list or any other static form of data that can be used as a reference point.

Hot-list Updates are manual or automated? Customizable real-time alerting based on specified criteria

Functionality to initiate certain actions based on real-time alert (sending email/text message, executing script etcetera)

**Notification**

- Does the product allow notification using SMS, Email, Pager, SNMP, API Integration etc?
- Is the Notification customizable?
- Does Notification workflow support the use of Templates to use Company logo, Header, Footer etc?
- Does it support multiple templates?

**Analyzing**

- Does the product allow analysts to drill down Rules, Events, Alerts easily?
- Does the product allow access to the raw event itself while investigating?
- Does the product allow users to perform Advanced Analysis - Statistical, Visual, Mathematical, empirical?
- Does the product allow Distributed search across multiple data stores?

**Reporting**

- Does the Solution provide graphical Business reporting using visual aids, graphics, dashboards, template based documents etcetera?
- How mature is the reporting capability? Matches or exceeds requirements?
- Ease of development of new reports, customization?
- How customizable is the reporting query?
- Does it have compliance packages to aid in compliance reporting?
- Automation of existing reports, tuning of generated reports, scheduling reports etcetera.
- How easy is the accessibility to internal, centralized log sources, in normalized and raw form in case of reporting needs?
- How varied and comprehensive is the Data export feature (extract logs, alerts, raw data etcetera.)? Does it support CSV, PDF, HTML, Raw text etcetera?
- Data Workflow Integration (Bidirectional access to information via external workflow tools?)

**8. Event Collection**

- Does the product have support for both Agent based Collection and Agent-less Collection?
- For Agent systems, does the solution support Windows, Unix and Linux Platforms, File readers, XML readers, Structured and unstructured data etcetera.
- For Agent-less, does the solution support Syslog, SNMP, SQL, ODBC/JDBC, and API collection
- Is the Agent management function centralized or is it standalone?
- Does it have any limitations in Input and Output Events Per Sec (EPS)?
- Does it offer the following capabilities to ensure reliability and flexibility?
  1. **Aggregation** - Can the Agent aggregate similar information based on custom defined grouping values defined by the System Administrator to cater to the changing Event Collection requirements?
  2. **Bandwidth Throttling** - Can the Agent prioritize forwarding of events based on defined values such as event priority? Can it send events at a specific bandwidth rate?
  3. **Filtering** - Can the agent provide Include as well as Exclude criteria for filtering?
  4. **Caching** - Can the agent cache all the events in the event that the Log Store goes
down? When forwarding the cache after failure does it intelligently throttle the events?

5. **Fail-over Capabilities** - Can the agent send Log events to a different alternate data store when the principal data store is down? Can it do multiple destination forwarding?

6. **Transport Integrity** - Can the agent encrypt the log transport to ensure confidentiality? What compression and encryption mechanisms are used?

7. **Health Monitoring** – Can the agent send health messages and statistics?

- For Microsoft Windows Event collection can the agent map the GUID/SUID to local registry/names/references for each event ID in the SYSTEM, SECURITY and all APPLICATION logs on the system?
- Are Agents that rely on Event Source Vendor API’s to connect and collect information approved and/or certified by that event source Vendor?
- Can the Agent follow dynamically changing folders and filenames? For example in order to support event sources like IIS Web Logs or custom applications that create a log per “site/application” per logging interval?
- Does the Agent support Database Administrator Logging (From both SQL and System / File Based Sources) for Oracle, MSSQL, MySQL and DB2?
- Agent parsing and mapping customization. Can the agent’s parsing be modified to assist with custom log messages? Can the normalization or categorization schema be updated to support custom log messages? How is system default functionality affected if these are modified?
- Can the Agent act as a NTP source for Source Event Logs or otherwise help in time synchronization for source event logs?
- Time difference adjustment feature (to allow the logging system to cope with devices having inconsistent times)

### 9. Conclusion

That is a long list of things to consider for SIEM Evaluation and we feel that there are many more items that go into the decision making process including Vendor relationships, Pricing, Value added services, etc. However, this guide is supposed to serve as a starting point for a Technical and Functional evaluation.