2015 Global Security Information and Event Management (SIEM) Enabling Technology Leadership Award
Contents
Background and Company Performance ................................................................. 3
   Industry Challenges ............................................................................................ 3
   Technology Leverage and Customer Impact ...................................................... 4
   Conclusion ........................................................................................................ 9
Significance of Enabling Technology Leadership .................................................. 10
Understanding Enabling Technology Leadership .................................................. 10
   Key Benchmarking Criteria .............................................................................. 11
Best Practice Award Analysis for LogRhythm Security Intelligence Platform .......... 11
   Decision Support Scorecard .......................................................................... 11
   Technology Leverage ....................................................................................... 12
   Customer Impact ............................................................................................. 12
   Decision Support Matrix .................................................................................. 13
The Intersection between 360-Degree Research and Best Practices Awards .......... 14
   Research Methodology .................................................................................... 14
About Frost & Sullivan ......................................................................................... 16
Background and Company Performance

Industry Challenges

Security information and event management (SIEM)\(^1\) is an indispensable technology for all organizations that have a significant information technology environment. SIEMs store and index for recall all events that occur on a network. The event management is granular and includes information about end-users, devices (IP and media access control (MAC) addresses), activities on infrastructure endpoints including servers, switches, and ports; the types of data flows on the network. Some SIEMs can process full packet capture (PCAP) of network traffic data.

Vertical markets and governments have specific industry compliance requirements. In November 2013, the Payment Card Industry Data Security Standard (PCI DSS) ratified its Rev 3.0 standard. The standard called for heightened security measures including audit trails linked to individual users as opposed to a generic process that can be linked back to individual users. As a part of The National Institute of Standards and Technology (NIST) standards, all federal government agencies must present a monthly inventory of all endpoints, operating systems, and applications within an agency’s network. Similar compliance requirements are prevalent in other industries. In a nutshell, SIEM is the most used technology for compliance reporting and auditing.

In the last three to four years, the SIEM vendors recognized their technology was under-utilized in the battle to protect cyber resources. Antivirus (AV), next generation firewalls (NGFW), intrusion detection/intrusion prevention systems (IDS/IPS), vulnerability management, and Web application scanners are technologies used to protect a network’s perimeter. Despite the efficacy of these platforms, miscreants still get in; systems get infiltrated (and then data gets exfiltrated).

SIEM is an integral part of the post-breach incident response process. If a system has been breached, an investigation is queued; and like criminal investigations, this process is known as forensics. The investigation must determine cause of the breach and the assets being targeted. The OS, a server type, users in an active directory, an application or device type are examples of attack targets. Additionally, the SIEM should be able to isolate and investigate activities based upon business, functional, or logical groupings.

The inclusion of advanced analytics can significantly truncate the post-breach incident response cycle; in fact, it is possible to detect anomalous behavioral traits before an attack detonates. A Chief Security Officer (CSO) can write rules that govern the SIEM, and if a rules violation occurs, an alarm can be sounded to prompt an investigation. Similarly, advanced analytics could be applied to establish statistical baselines. If an endpoint is

\(^1\) In this award citation Frost & Sullivan is considering SIEM and log management (LM) to be congruent technologies. When the term SIEM is used, this is also meant to include information coming from logs, and how logs are managed on the same platform.
ingesting or expelling an inordinate amount of data, or if a data type that has never been accessed by an endpoint (perhaps a peer-to-peer Tor application, for example) is introduced to the network, an alarm can be sounded.

SIEM is both art and science. The use cases just mentioned are common for enterprise-level clients, but separating noise from meaningful data is a considerable task. Finding and then presenting meaningful data in such a way that the data becomes actionable is the fruition of SIEM technology.

**Technology Leverage and Customer Impact**

SIEM may appear on the surface as a singular, integrated technology, but it is actually a combination of many discrete elements of a technology done well. How these elements are executed in concert with one another is a key differentiator. The best SIEMs excel in search functions, rules generation, compliance reporting, log management, network monitoring, and forensics. Interactive dashboards help to automate future incident investigations, and advanced analytics scan data logs and network telemetry to find indications of compromise (IOC).

The Enabling Technology Leadership Award is how Frost & Sullivan recognizes new best-of-breed technologies. In this citation, Frost & Sullivan recognizes how LogRhythm differentiates its SIEM functionality; but as importantly how LogRhythm combines the discrete elements of SIEM to create a better user experience and reduce mean-time-to-detection and mean-time-to-respond to incidents for better threat mitigation and remediation.

**Commitment to Innovation**

To enhance their SIEM offerings, many vendors choose to “bolt-on” advanced functionality into existing platforms in the name expediently getting the feature to market rather than taking the time to provide a seamless integration. The LogRhythm Security Intelligence Platform, however, was integrated directly into the SIEM. LogRhythm’s AI Engine provides the logistics in the Security Intelligence Platform. LogRhythm archives unaltered, non-normalized logs for regulatory compliance and for legal and investigative purposes. Even at the data flow collection stage, the AI Engine is applying advanced correlations and behavioral analytics to identify suspicious or anomalous behavior. While the collection of anomalous behavior gets a significant amount of attention, the same analytics also create behavioral whitelists of “normal” activity. Whitelisting helps to negate the number of false positives by delivering more accurate, exception-based alerting.

The next generation SIEM is an integral part of a continuous network monitoring security posture. The word “continuous” becomes a practical concern as any poorly designed function becomes a road block, such as:
• **Search.** The search function has to be intuitive. The search engine has to enable the CSO to build conditional statements into the search.

• **Intelligent Indexing.** At the time of ingestion, data has to be segmented for storage, future searches, and investigation.

• **Advanced Correlation and Pattern Recognition.** Establishing statistical baselines and understanding known behaviors is important in anomaly detection, and, in recognizing good behavior for whitelisting.

• **Network Visibility.** Advanced analytics, search functions, and rule-writing can only be effective within the context of how a network is designed and the data usage pattern of end-users. In a SIEM, network visibility is not an active element like an NMAP. Rather, network visibility occurs as the collection of application logs, router logs, network telemetry, and server logs.

• **Compliance Auditing and Reporting.** The historical use case for SIEM remains a differentiator in SIEM. In the best case scenarios, compliance reporting is designed for the CSO so that the CSO can take measures to improve the compliance posture of his network, and satisfy the needs of auditors.

• **Machine learning.** SIEM platforms need to be able to provide different degrees of automation in search, and in incident response. Additionally, an analytical engine should be fine-tuned when in use to establish better statistical baselines, and to create profiles of normal behavior.

The LogRhythm architecture treats each SIEM function as an integrated process. Search and Intelligent Indexing are tightly correlated. Advanced correlation cannot happen without visibility of all network infrastructure and end-use devices. The ability to transition between SIEM functions directly effects the mean-time-to-detect and mean-time-to-respond to cyber-threats.

**Commitment to Creativity**

SIEMs have tremendous value as a way to log events. An “event” is a seemingly benign term used to describe any piece of data ingested in a SIEM. Ordinary network telemetry, communications between IP and MAC addresses, and server and router logs are examples of events.

Like snowflakes, no two events are alike—each event has its own unique characteristics. Time is an indelible characteristic; each event happens at a specific time. Data consumption can be recorded as can application usage. All information is potentially an actionable event—LogRhythm demonstrates creativity and expertise in turning event management into an integral part of a continuous cyber-network defense.
The following figure shows three phases of analytics for threat detection and mitigation in the LogRhythm Security Intelligence Platform.

Figure 1    LogRhythm Analytics-Driven Defense

Historically, SIEM engines have been built to ingest as much data as possible. Recently, advanced analytics are being used for network behavior anomaly detection (NBAD). At the time of data ingestion, a data segmentation process takes place. LogRhythm offers Intelligent Indexing. Intelligent Indexing determines which data is the most valuable. Determining what goes into hot storage and what can be archived is the first protocol. Establishing data hierarchy ensures that the most important data is immediately accessible for reports, investigations and live tails. Data that is designated as important for trending is stored in LogMart, which is LogRhythm’s online long term data warehouse.

SIEMs use a rules-based mechanism. If a rule is violated, the CSO can be notified. Alarms can also be sounded if network anomalies are detected, behavioral analytics detect a change in end-user behavior, or if known statistical baseline thresholds are surpassed. Depending upon the severity of the alarm, an investigation may be initiated.

Like rules-writing, the search function is vitally important for SIEM products. SIEM platforms are used for compliance auditing and reporting, used to begin forensics investigations, and (hopefully) find IoC before data exfiltration; all of these functions are heavily reliant on search. Search is effectively a two pronged process. Data has to be stored in such a way as facilitate the search function (as described by Intelligent Indexing), and then the search itself must be effective.

The search engine should be intuitive and easy to use. The interface on the LogRhythm Security Intelligence Platform dashboard is interactive: any event (applications, data flow,
and end-user history are examples) can be drilled down into or pivoted from for purposes of monitoring or toward formal investigations.

Customizable widgets and dashboards facilitate the search function. As each new analytics criterion is selected, a "breadcrumb" is created to create an intuitive display of all search and filter criteria. Each breadcrumb can be studied separately. If a CSO prefers, a command-line approach can use the Lucene query language to perform complex searches.

The last part of the incident response is to begin the process of threat mitigation. In the LogRhythm Security Intelligence Platform this process is known as SmartResponse. SIEMs communicate bidirectionally with other cyber-security platforms to enhance the efficacy of each. As a part of SmartResponse and in conjunction with partner alliances, if the SIEM detects anomalous behavior, an instruction can be sent to IDS/IPS to block access to network, or to a NAC to send an end-user to a different part of the network.

Many organizations remain reluctant to fully automate responses to threats. The SmartResponse remediation response includes an optional, built-in approval process that can require up to three levels of authorization prior to taking action.

**Commercialization Success**

LogRhythm is rapidly ascending into a global SIEM leadership position. Frost & Sullivan estimates the 2014 global SIEM revenue market to be worth more than $1.5 billion. SIEM products are offered by the most renowned multi-national companies in network security.

LogRhythm is establishing footholds in all markets. Enterprise customers purchase the LogRhythm SIEM for its combination of strong analytics and compliance and auditing platforms. To win enterprise customers, the SIEM must be horizontally and vertically scalable to accommodate massive data requirements and multiple locations. For small-to-midsized businesses (SMB), LogRhythm offers an all-in-one appliance that includes the event manager, the log manager, and the AI Engine.

Frost & Sullivan estimates LogRhythm had better than 50% year-over-year growth in both 2013 and 2014. Currently, LogRhythm is the sixth-largest global SIEM vendor and has better revenue growth rates than any other major SIEM vendor.

**Price/Performance Value**

LogRhythm offers the Enterprise Licensing Program (ELP) for larger accounts. Recognizing that enterprises are likely to have multiple locations; pricing is based on messages per second (MPS), not on the number of appliances installed. Additionally, the MPS calculation is based upon a 24-hour rolling average as opposed to peak-usage. The ELP license ensures the client does not pay extra for software, collection, and system monitoring licensing costs.
Of course, when companies purchase network security platforms, the operational cost includes the salaries of highly trained personnel. SIEM platforms are not easy to activate. The SIEM vendor can make the experience less painful (and less costly) with smart integrations, and intuitive tools. Toward that end, the following are tools LogRhythm offers:

- **The LogRhythm Installer.** The installation tool can install and/or upgrade all components through a single interface and is available for both appliances and software deployments.

- **Active Directory Group Based Authorization.** This feature set is a direct integration to the SIEM that allows customers to use their active directory infrastructure to automatically provision and manage LogRhythm user accounts.

- **Data Management Profiles.** Configuring servers to conform to a company’s data delivery system is time-consuming and difficult. The Data Management Profile Wizard delivers standardized configuration options for various data management modes based on best practices for customer requirements.

- **System Monitor Agent.** LogRhythm utilizes agents for both log collection as well as for network monitoring including file integrity monitoring. The registration process allows for quick agent deployment and recognition with centralized, batch administration. The System Monitor Agent also configures agents in minutes.

LogRhythm is building a strong reputation as its SIEM is built for the needs of its customer-base and much of the operating overhead that can be a part of working with a SIEM is reduced in architecture, integration, usability and in feature sets.

**Customer Ownership Experience**

The implementation of rules engines can add hidden costs and unforeseen effort to the purchase and activation a new SIEM solution. The LogRhythm Security Intelligence Platform offers extensive out-of-the box rules settings for vertical markets, drastically improving the implementation experience for the customer. LogRhythm’s compliance automation suites are updated automatically and include over 1,100 reports, alerts, and investigations aligned directly with specific compliance mandates and security best practices.

Clients fully expect that platforms evolve to incorporate new compliance standards or to include new threat exchange information. Knowledge Base Modules are available for specific regulatory compliance and general security needs and updates are delivered regularly; at a minimum of every other week. Additionally, functional security use cases such as NBAD, Web application defense, privileged user monitoring and advanced persistent threat (APT) detection, and other operational modules, are frequently updated.
While many SIEM platforms are capable of PCAP, the cost of storing and recalling full-packets of data is prohibitive. However, investigating full packets is the best resolution for an incident response. LogRhythm developed a proprietary technology that addresses the dilemma. SmartCapture, a feature in Network Monitor, is used to pare down the heavy payload requirements of PCAP. Using the real-time rules engine as a guide, SmartCapture determines “sessions of interest” based upon application type or association with concerning events. Only full-packets in “sessions of interest” are permanently logged.

A SIEM vendor augments his appliance or service with a strong support staff and customer service. Often customers need support in configurations or in the development of custom API to link programs and applications to the SIEM. LogRhythm is expanding current relationships and winning new business by becoming a technical partner to companies as well as a security platform provider.

**Conclusion**

Once thought of as a repository of data and a compliance auditing and reporting appliance, SIEMs now add another security measure to detect the evasion of cyber defenses. The SIEM has become the platform that enhances and binds other cybersecurity platforms allowing clients to build a multilayered cyber-defense. Advanced analytics and the establishment of statistical baselines are required to see where a network might otherwise be unstable. The ability of the SIEM to establish rules and to index data for optimal correlation and recall is on par with applied analytics. LogRhythm has a superior platform in the strength of its integrated analytics and in how each feature set leads into a better end-user experience.

With its strong overall performance, LogRhythm has earned Frost & Sullivan’s 2015 Enabling Technology Leadership Award.
Significance of Enabling Technology Leadership

Ultimately, growth in any organization depends upon customers purchasing from your company, and then making the decision to return time and again. In a sense, then, everything is truly about the customer—and making those customers happy is the cornerstone of any long-term successful growth strategy. To achieve these goals through technology leadership, an organization must be best-in-class in three key areas: understanding demand, nurturing the brand, and differentiating from the competition.

Understanding Enabling Technology Leadership

Product quality (driven by innovative technology) is the foundation of delivering customer value. When complemented by an equally rigorous focus on the customer, companies can begin to differentiate themselves from the competition. From awareness, to consideration, to purchase, to follow-up support, best-practice organizations deliver a unique and enjoyable experience that gives customers confidence in the company, its products, and its integrity.
Key Benchmarking Criteria

For the Enabling Technology Leadership Award, Frost & Sullivan analysts independently evaluated two key factors—Technology Leverage and Customer Impact—according to the criteria identified below.

Technology Leverage
- Criterion 1: Commitment to Innovation
- Criterion 2: Commitment to Creativity
- Criterion 3: Stage Gate Efficiency
- Criterion 4: Commercialization Success
- Criterion 5: Application Diversity

Customer Impact
- Criterion 1: Price/Performance Value
- Criterion 2: Customer Purchase Experience
- Criterion 3: Customer Ownership Experience
- Criterion 4: Customer Service Experience
- Criterion 5: Brand Equity

Best Practice Award Analysis for LogRhythm Security Intelligence Platform

Decision Support Scorecard

To support its evaluation of best practices across multiple business performance categories, Frost & Sullivan employs a customized Decision Support Scorecard. This tool allows our research and consulting teams to objectively analyze performance, according to the key benchmarking criteria listed in the previous section, and to assign ratings on that basis. The tool follows a 10-point scale that allows for nuances in performance evaluation; ratings guidelines are illustrated below.

RATINGS GUIDELINES

The Decision Support Scorecard is organized by Technology Leverage and Customer Impact (i.e., the overarching categories for all 10 benchmarking criteria; the definitions for each criteria are provided beneath the scorecard). The research team confirms the veracity of this weighted scorecard through sensitivity analysis, which confirms that small
changes to the ratings for a specific criterion do not lead to a significant change in the overall relative rankings of the companies.

The results of this analysis are shown below. To remain unbiased and to protect the interests of all organizations reviewed, we have chosen to refer to the other key players as Competitor 2 and Competitor 3.

DECISION SUPPORT SCORECARD FOR ENABLING TECHNOLOGY LEADERSHIP AWARD

<table>
<thead>
<tr>
<th>Measurement of 1–10 (1 = poor; 10 = excellent)</th>
<th>Technology Leverage</th>
<th>Customer Impact</th>
<th>Average Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enabling Technology Leadership</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LogRhythm</td>
<td>9.6</td>
<td>9.6</td>
<td>9.6</td>
</tr>
<tr>
<td>Competitor 2</td>
<td>8.3</td>
<td>8.1</td>
<td>8.2</td>
</tr>
<tr>
<td>Competitor 3</td>
<td>8.5</td>
<td>7.7</td>
<td>8.1</td>
</tr>
</tbody>
</table>

**Technology Leverage**

**Criterion 1: Commitment to Innovation**
Requirement: Conscious, ongoing adoption of emerging technologies that enables new product development and enhances product performances

**Criterion 2: Commitment to Creativity**
Requirement: Technology is leveraged to push the limits of form and function, in the pursuit of "white space" innovation

**Criterion 3: Stage Gate Efficiency**
Requirement: Adoption of technology to enhance the stage gate process for launching new products and solutions

**Criterion 4: Commercialization Success**
Requirement: A proven track record of taking new technologies to market with a high rate of success

**Criterion 5: Application Diversity**
Requirement: The development and/or integration of technologies that serve multiple applications and can be embraced in multiple environments

**Customer Impact**

**Criterion 1: Price/Performance Value**
Requirement: Products or services offer the best value for the price, compared to similar offerings in the market

**Criterion 2: Customer Purchase Experience**
Requirement: Customers feel like they are buying the most optimal solution that addresses both their unique needs and their unique constraints
**Criterion 3: Customer Ownership Experience**
Requirement: Customers are proud to own the company’s product or service, and have a positive experience throughout the life of the product or service

**Criterion 4: Customer Service Experience**
Requirement: Customer service is accessible, fast, stress-free, and of high quality

**Criterion 5: Brand Equity**
Requirement: Customers have a positive view of the brand and exhibit high brand loyalty

**Decision Support Matrix**
Once all companies have been evaluated according to the Decision Support Scorecard, analysts can then position the candidates on the matrix shown below, enabling them to visualize which companies are truly breakthrough and which ones are not yet operating at best-in-class levels.

DECISION SUPPORT MATRIX FOR ENABLING TECHNOLOGY LEADERSHIP AWARD

![Decision Support Matrix Diagram]
The Intersection between 360-Degree Research and Best Practices Awards

Research Methodology

Frost & Sullivan’s 360-degree research methodology represents the analytical rigor of our research process. It offers a 360-degree-view of industry challenges, trends, and issues by integrating all 7 of Frost & Sullivan's research methodologies. Too often, companies make important growth decisions based on a narrow understanding of their environment, leading to errors of both omission and commission. Successful growth strategies are founded on a thorough understanding of market, technical, economic, financial, customer, best practices, and demographic analyses. The integration of these research disciplines into the 360-degree research methodology provides an evaluation platform for benchmarking industry players and for identifying those performing at best-in-class levels.
Best Practices Recognition: 10 Steps to Researching, Identifying, and Recognizing Best Practices

Frost & Sullivan Awards follow a 10-step process to evaluate award candidates and assess their fit with select best practice criteria. The reputation and integrity of the Awards are based on close adherence to this process.

<table>
<thead>
<tr>
<th>STEP</th>
<th>OBJECTIVE</th>
<th>KEY ACTIVITIES</th>
<th>OUTPUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Monitor, target, and screen</td>
<td>Identify award recipient candidates from around the globe</td>
<td>Conduct in-depth industry research • Identify emerging sectors • Scan multiple geographies</td>
</tr>
<tr>
<td>2</td>
<td>Perform 360-degree research</td>
<td>Conduct comprehensive, 360-degree research on all candidates in the pipeline</td>
<td>Interview thought leaders and industry practitioners • Assess candidates’ fit with best-practice criteria • Rank all candidates</td>
</tr>
<tr>
<td>3</td>
<td>Invite thought leadership in best practices</td>
<td>Perform in-depth examination of all candidates</td>
<td>Confirm best-practice criteria • Examine eligibility of all candidates • Identify any information gaps</td>
</tr>
<tr>
<td>4</td>
<td>Initiate research director review</td>
<td>Conduct an unbiased evaluation of all candidate profiles</td>
<td>Brainstorm ranking options • Invite multiple perspectives on candidates’ performance • Update candidate profiles</td>
</tr>
<tr>
<td>5</td>
<td>Assemble panel of industry experts</td>
<td>Present findings to an expert panel of industry thought leaders</td>
<td>Share findings • Strengthen cases for candidate eligibility • Prioritize candidates</td>
</tr>
<tr>
<td>6</td>
<td>Conduct global industry review</td>
<td>Build consensus on award candidates’ eligibility</td>
<td>Hold global team meeting to review all candidates • Pressure-test fit with criteria • Confirm inclusion of all eligible candidates</td>
</tr>
<tr>
<td>7</td>
<td>Perform quality check</td>
<td>Develop official award consideration materials</td>
<td>Perform final performance benchmarking activities • Write nominations • Perform quality review</td>
</tr>
<tr>
<td>8</td>
<td>Reconnect with panel of industry experts</td>
<td>Finalize the selection of the best-practice award recipient</td>
<td>Review analysis with panel • Build consensus • Select winner</td>
</tr>
<tr>
<td>9</td>
<td>Communicate recognition</td>
<td>Inform award recipient of award recognition</td>
<td>Present award to the CEO • Inspire the organization for continued success • Celebrate the recipient’s performance</td>
</tr>
<tr>
<td>10</td>
<td>Take strategic action</td>
<td>Upon licensing, company may share award news with stakeholders and customers</td>
<td>Coordinate media outreach • Design a marketing plan • Assess award’s role in future strategic planning</td>
</tr>
</tbody>
</table>
About Frost & Sullivan

Frost & Sullivan, the Growth Partnership Company, enables clients to accelerate growth and achieve best in class positions in growth, innovation and leadership. The company's Growth Partnership Service provides the CEO and the CEO's Growth Team with disciplined research and best practice models to drive the generation, evaluation and implementation of powerful growth strategies. Frost & Sullivan leverages almost 50 years of experience in partnering with Global 1000 companies, emerging businesses and the investment community from 31 offices on six continents. To join our Growth Partnership, please visit http://www.frost.com.