DCIG 2014-15 Security Information and Event Management (SIEM) Appliance Buyer's Guide Now Available

DCIG is pleased to announce the availability of its DCIG 2014-15 Security Information and Event Management (SIEM) Appliance Buyer's Guide. In this Buyer's Guide, DCIG weights, scores and ranks 29 SIEM appliances respectively from nine (9) different providers. Like all previous DCIG Buyer's Guides, this Buyer's Guide provides the critical information that all size organizations need when selecting a SIEM appliance to help provide visibility into their security posture by providing usable and actionable information.

Data security is a part of the IT infrastructure that should take care of itself. Companies have enough to worry about without always looking over their shoulder to make sure no one is stealing vital information.

As most organizations recognize, this is *NOT* the case. Security specialists are rarely without work for the simple reason that almost every day a headline reads *"International Company [you fill in the blank] Suffers Massive Data Breach."* Read deeper into those articles and a company representative

is often quoted as saying something akin to, *"The breach happened a couple days ago and we just caught it. We're still trying to figure out how many of our customers were affected and who is responsible."*

The truth of the matter is that data security does not take care of itself. But SIEM solutions take the edge off of these concerns by acting as a constant watchdog that perform several services:

- Logging information
- Correlating data
- Alerting security administrators as soon as a breach is detected
- Providing a dashboard to provide a picture of what is happening in the environment at any given time

SIEM solutions and the dashboards they offer put a big dent in addressing that problem. When a breach is detected, an administrator can pull up a dashboard that breaks down every user session that has taken place by login name, location, applications launched, and more. Using these dashboards, the security administrator can make short work of finding those responsible.

This information is presented in easily accessible charts and lists that can be used for personal protection and also for forensic investigations should the need arise. Further, they may be shown to potential customers worried about security and who want proof that the company is doing everything it can to protect and secure their data.

Every SIEM appliance contained in the *DCIG 2014-15 SIEM Appliance Buyer's Guide* performs the following primary functions:

1. Data and log aggregation
2. Data correlation
3. Alerting

4. Dashboarding
5. Log and data retention and protection.

Many also perform three (3) secondary functions:

1. Forensic analysis on the information
2. Serve as an incident management tool
3. Perform compliance monitoring

It is important that prospective buyers keep in mind their organization's security requirements as they look to acquire one of these SIEM appliances. What might be the best SIEM solution for a large, international company might be too robust for a smaller organization. A company must be aware of its own security needs before investing time and money in an SIEM solution.

It is in this context that DCIG presents the DCIG 2014-15 SIEM Appliance Buyer's Guide. As prior Buyer's Guides have done, this Buyer's Guide puts at the fingertips of organizations a comprehensive list of SIEM appliances and the features they offer in the form of detailed, standardized data sheets that can assist them in this important buying decision.

This *DCIG 2014-15 SIEM Appliance Buyer's Guide* accomplishes the following objectives:

- Provides an objective, third party evaluation of SIEM solutions that weights, scores and ranks their features from an end user's viewpoint
- Includes recommendations on how to best use this Buyer's Guide
- Scores and ranks the features on each SIEM appliance based upon criteria that matter most to end users so they can quickly know which products are the most appropriate for them to use and under what conditions
- Provides data sheets for 29 SIEM appliances from nine (9) different providers so end users can do quick comparisons of the features that are supported and not

supported on each product
- Gives any organization the ability to request competitive bids from different providers of SIEM appliances to do *apples-to-apples* comparisons of these products

The DCIG 2014-15 SIEM Appliance Buyer's Guide Top 10 solutions include (in alphabetical order):

- BlackStratus MIDWAY
- Hewlett-Packard ArcSight AE-7526
- Hewlett-Packard ArcSight AE-7566
- Hewlett-Packard ArcSight AE-7581
- IBM Security QRadar SIEM 3105
- IBM Security QRadar SIEM 3124
- LogRhythm All-in-One (XM) 4300
- LogRhythm All-in-One (XM) 4300
- McAfee ETM-6000
- TIBCO LogLogic MX4025

The **LogRhythm All-in-One** (XM) 6300 SIEM appliance achieved the *Best-in-Class* ranking in this inaugural *DCIG 2014-15 SIEM Appliance Buyer's Guide.* Scoring at or near the top in every category (Hardware, Software, Management and Support) evaluated in this Buyer's Guide, it represents the best of what SIEM appliances currently have to offer.

In doing its research for this Buyer's Guide, DCIG uncovered some interesting statistics about SIEM appliances in general:

- 100% include log management, application monitoring and audit report capabilities
- 90% provide some type of RAID configuration
- 79% of appliances provide the ability to export data as comma separated values (CSV)
- 72% support distributed searches across multiple data stores
- 58% can achieve maximum event processing rates of 2,500

EPS
- 24% can provide logging or monitoring on more than 2000 systems
- 21% offer 10 TB or more of storage capacity on their appliance

The DCIG 2014-15 SIEM Appliance Buyer’s Guide is immediately available through the DCIG analyst portal for subscribing users by following this link.