

SIEM Presentation to AOA IT

Sunday, January 8, 2012

Eumi Sprague
Information Technology
Cal Poly Corporation
San Luis Obispo, CA



What is SIEM?

Security Information and Event Management

- ❑ Security Information Management (SIM)
 - Log Management and Compliance Reporting
- ❑ Security Event Management (SEM)
 - Real-time Monitoring and Incident Management for Security-related Events from Networks, Security Devices, Systems, and Applications

Source: Gartner 2011 Magic Quadrant for SIEM

What is SIEM – cont'd

SIEM Technology:

- ❑ Compliance – Log Management and Compliance Reporting
- ❑ Threat Management – real time monitoring of user activity, data access, application activity, and incident management
- ❑ A deployment that provides a mix of compliance and threat management capabilities



SIEM - Our Story

- What we did
- Where we are
- Where we are headed



What We Did

- ❑ Our journey began about 18 months...
- ❑ Sampled Two Systems
 - LogRhythm
 - TriGeo (now called SolarWinds)
- ❑ Budgeted for Purchase in FY2011-12

What We Did – cont'd

- Find out what others were using
 - Cal Poly, SLO, use Splunk (open source)
 - AOA IT Forum
 - ✓ No responses posted on the IT forum
 - Check List Servs:
 - ✓ SECURITY@LISTSERV.EDUCAUSE.EDU
 - ✓ PCI-COMPLIANCE@LISTSERV.UARK.EDU

Excellent PCI List Serv. By invitation only. Email Chrissy Woodward at cwoodwa@uark.edu to be added.

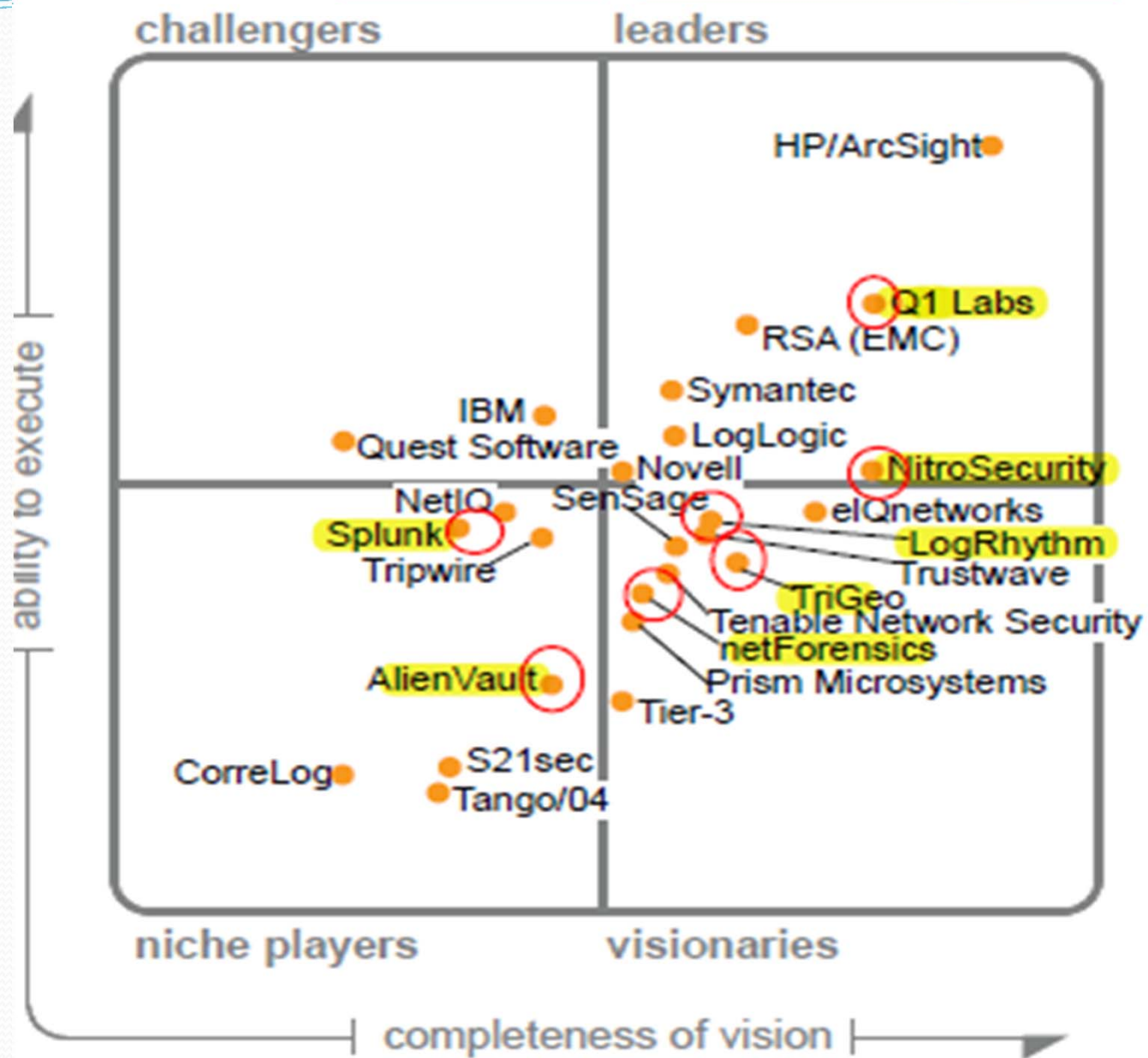
Summary of List Serv Results – page 1

No.	Institution	System	Note
1	Utah State University	OSSEC (www.ossec.net), Splunk (www.splunk.com)	Open Source
2	Canisius College, Buffalo, NY	OSSIM (http://alienvault.com)	Open Source
3	St. Clout State, St. Cloud, MN	LogRhythm (www.logrhythm.com)	
4	Central Piedmont Community College, Charlotte, NC	OSSSEC (www.ossec.net)	Open Source
5	Florida State Univ, Tallahassee, FL	NitroSecurity (ESM) www.nitrosecurity.com	

Summary of List Serv Results – page 2

No.	Institution	System	Note
6	Purdue University	Enterasys Networks (www.enterasys.com)	
7	Norfolk State Univ, Norfolk, VA	Nitro Security www.nitrosecurity.com	
8	The University of Oklahoma HSC, Oklahoma City, OK	Net Forensics www.netforensics.com	
9	College of Western Idaho, Nampa, ID	LogRhythm www.logrhythm.com	

Gartner's 2011 SIEM Magic Quadrant



Open Source Systems

- ❑ Options
 - OSSEC www.ossec.net
 - Splunk www.splunk.com
 - OSSIM <http://alienvault.com/>

- ❑ Pros
 - Less cost

- ❑ Cons
 - Not as robust as the commercial systems
 - Requires more work to deploy



Where We Are

- ❑ Look at LogRhythm & Solarwinds again
- ❑ Look at Q1Labs
 - Used by Juniper Labs
 - Cost will be an important factor
- ❑ Review and evaluate systems
- ❑ Select a system



Where We are Headed

- ❑ Implement a System
- ❑ Time Line → within 6 to 12 months



Conclusion –

- ❑ SIEM market has matured
- ❑ Many systems to choose from
- ❑ Wealth of information available
- ❑ Helps to know our requirements
- ❑ Implementation is the new beginning
- ❑ Need to manage the information
- ❑ Would love to collaborate...