WELCOME: CROSSOVER MEETING

SEA-TUG

ISSA
Information Systems Security Association
New Hampshire Chapter

Wednesday, September 20, 2017

SEA-TUG

bringing IT together℠

ABOUT SEA-TUG

- Founded in 2001 by Rob Bergin and Steve Noel to help IT professionals in the seacoast collaborate and enhance their knowledge
- New steering committee formed July 2016
  - John Whelan, Pamela Capper, Deb Gale, PJ Soucy, Joel Wright, Derek Rolfe, Rob Maciorski, Terry Jamro, Chris Morris
- Part of larger user group communities
  - Boston User Groups, Meetup, etc.

ABOUT ISSA NH

- ISSA® is an international organization providing educational forums, publications, and peer interaction opportunities that enhance the knowledge, skills, and professional growth of its information security professional members
- The primary goal of ISSA is to promote best practices that will ensure availability, integrity, and security of organizational resources
- Since its inception in 1982, ISSA's membership has grown to include more than 100 chapters around the world
- NH Chapter: Scot Sakelarios, Todd Waskelis, Charles Roy II, Scott Finkelstein

This is YOUR user group – help us make it better. What topics do you want covered?

SEA-TUG

bringing IT together℠

Thank you to…

- Alexander Technology Group
  - Food/beverages
  - http://www.alexandertg.com
- Great Bay Community College
  - Meeting space
- Axis Business Solutions
  - ISSA NH General Sponsor
  - http://axisbusiness.com

bringing IT together℠

Tonight's Presentation

Managing Log Data

How to Leverage a SIEM

Jason Sgro – Chief Strategist, The ATOM Group

Data Is the Answer

(What was the Question?)

Michael Leland – SIEM Evangelist, McAfee/Intel

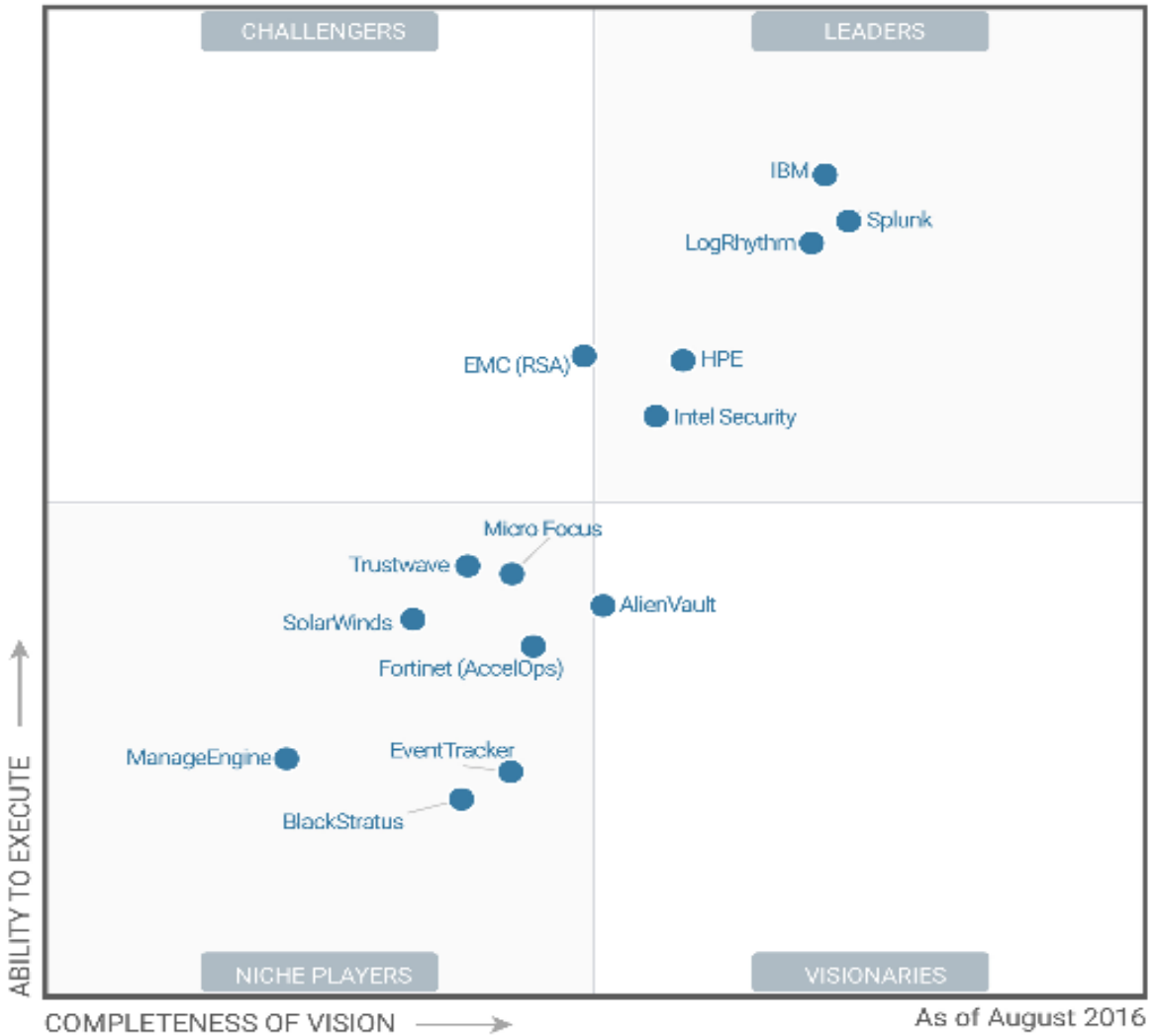
SEA-TUG

bringing IT together℠

Don’t deploy a SIEM unless you can commit at least 20 hours per week to it.

- SIEMonster
- Alienvault
- EventSentry
- Elk/Graylog
- Logly
- Arcsight
- QRadar
- Splunk
- Exabeam
- Logrythm
- Trustwave
- LogLogic
- Mcafee ESM
- RSA
- FortiSIEM
- Solarwinds LEM
- NNT LogTracker
- NetIQ Sentinel
- Logpoint
- ManageEngine

Figure 1. Magic Quadrant for Security Information and Event Management



Or engage an MSSP to manage the system

- Pervade
- SecureWorks
- Rapid7
- RedCanary
- IBM
- AT&T
- Symantec
- Trustwave
- Verizon
- Atos
- Guardant
- TruSecure
- Integralis
- EIQ
- NetSwitch
- Many More