Protect 2014

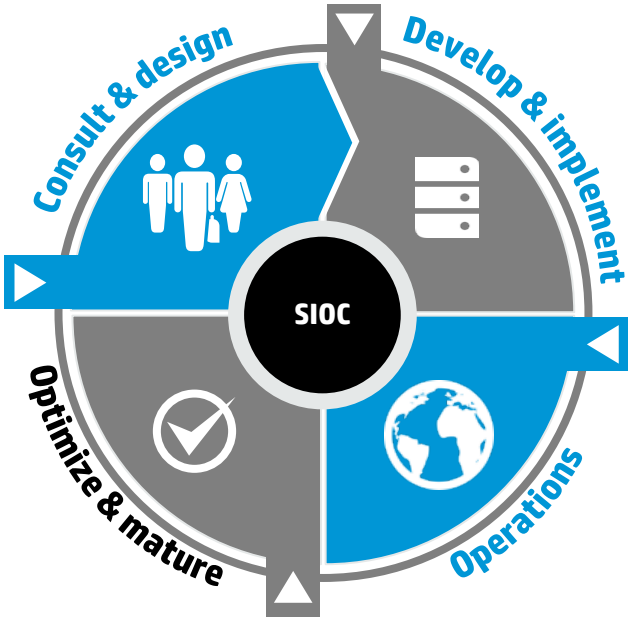
Washington, D.C. September 8-11

State of Security Operations

Roberto Sandoval / September 2014

Security Intelligence & Operations Consulting

Founded: 2007



hp.com/go/sioc

The best in the world at building state of the art security operations capabilities/cyber defense programs.

Experience

- 35+ SOC builds
- 100+ SOC assessments
- 30+ SIOC consultants worldwide
- Over 100 years of cumulative SOC experience

Solution approach

- People, process & technology

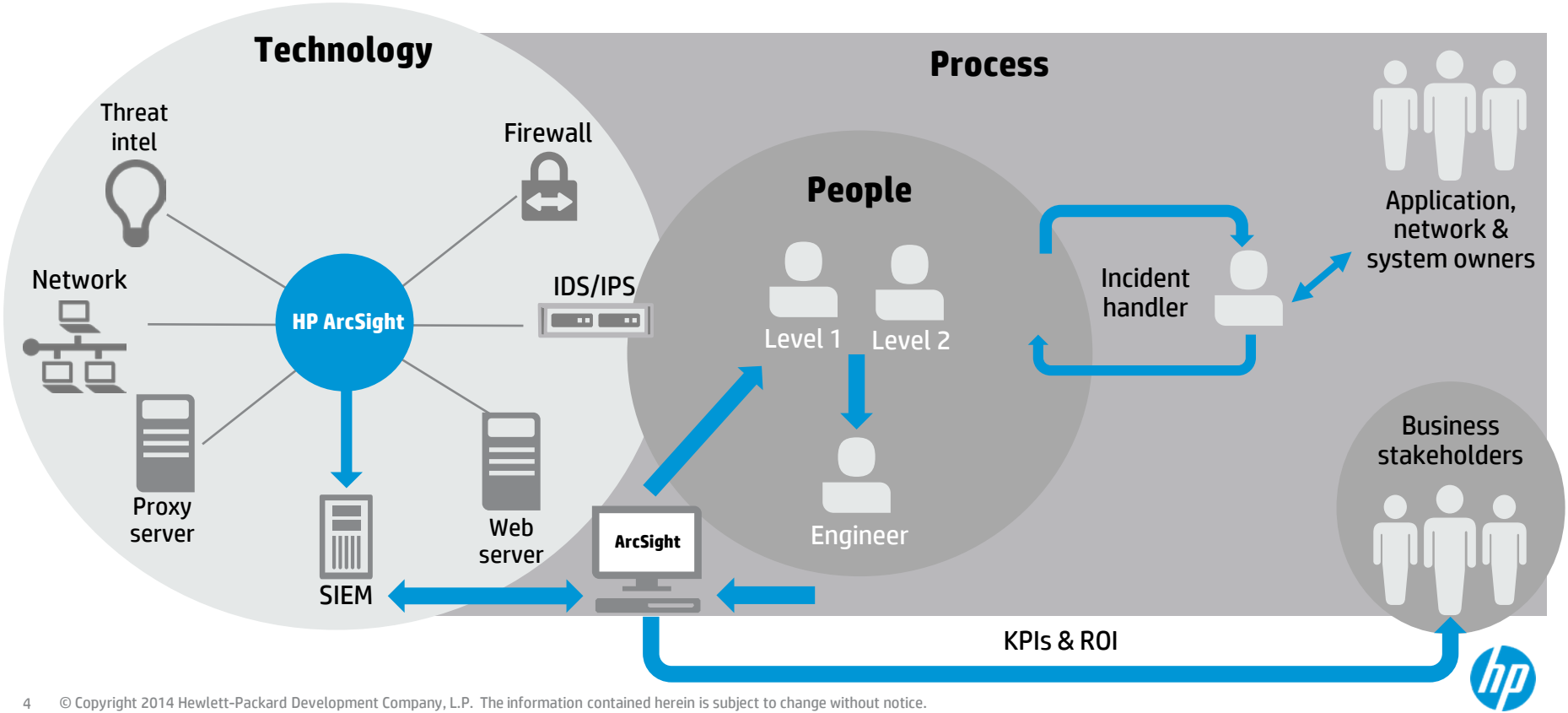
Accelerated success

- Mature project methodology
- Best practices
- Extensive intellectual capital

State of Security Operations 2014

- Publish date: January 28, 2014
- First-of-its-kind industry report
- Based on 5 years of assessment data
- -93 assessments performed in 13 countries
- Key findings
- Customer examples
- Industry-specific statistics and findings
- Assessment methodology
  - **People, process, technology, and business**

Assessment scope



Assessment methodology

- Mission
- Accountability
- Sponsorship
- Relationship
- Deliverables
- Vendor engagement
- Facilities

- Training
- Certifications
- Experience
- Skill assessments
- Career path
- Leadership

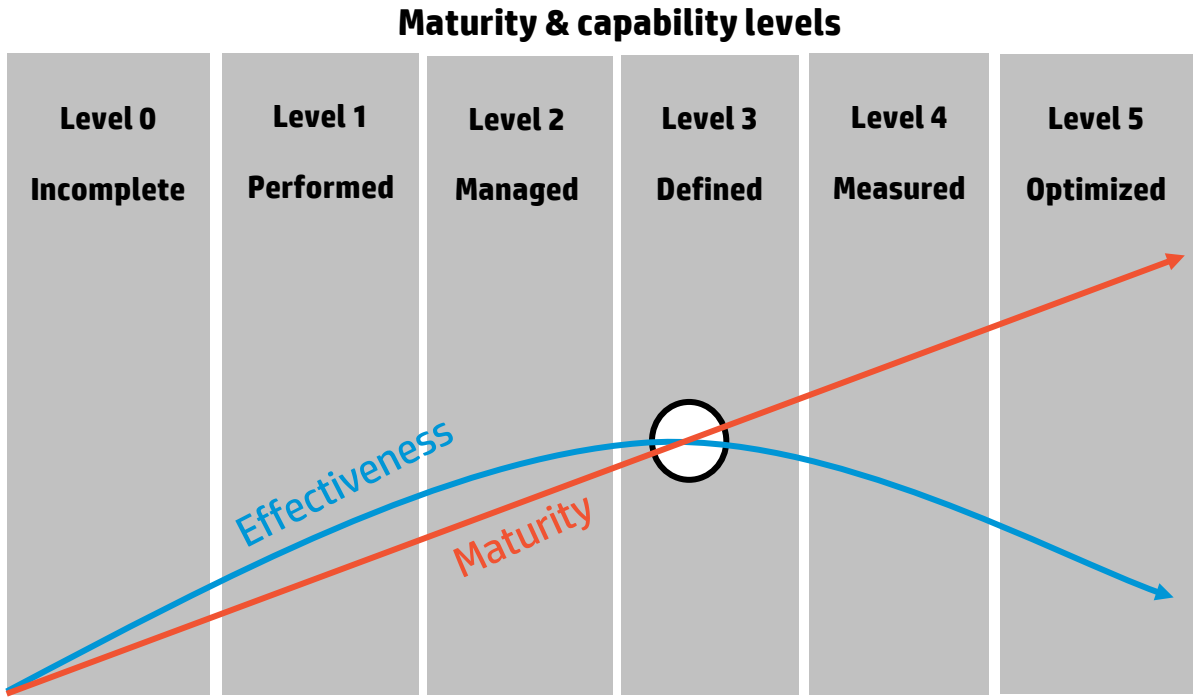
- Operational processes
- Analytical processes
- Business processes
- Technology processes

- Architecture
- Data collection
- Monitoring
- Correlation
- Infrastructure planning

Maturity and capability levels

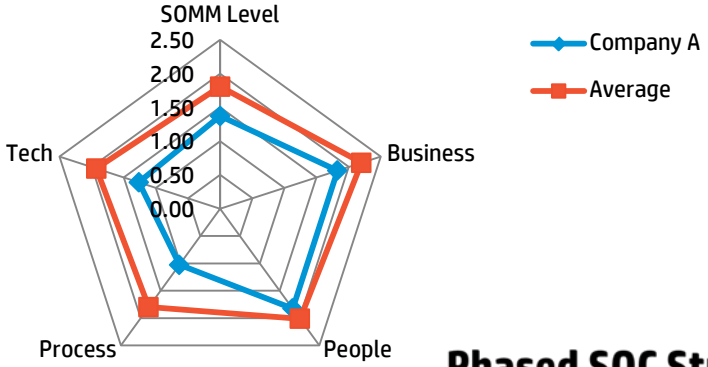
Assessment methodology

- Quantitative assessment of business, people, process and technology
- Based on Carnegie Mellon – *Software Engineering Institute's - Capability Maturity Model for Integration* (SEI-CMMI)
- Year-to-year trends and comparisons across industries



SOC Discovery Assessment

Industry comparison



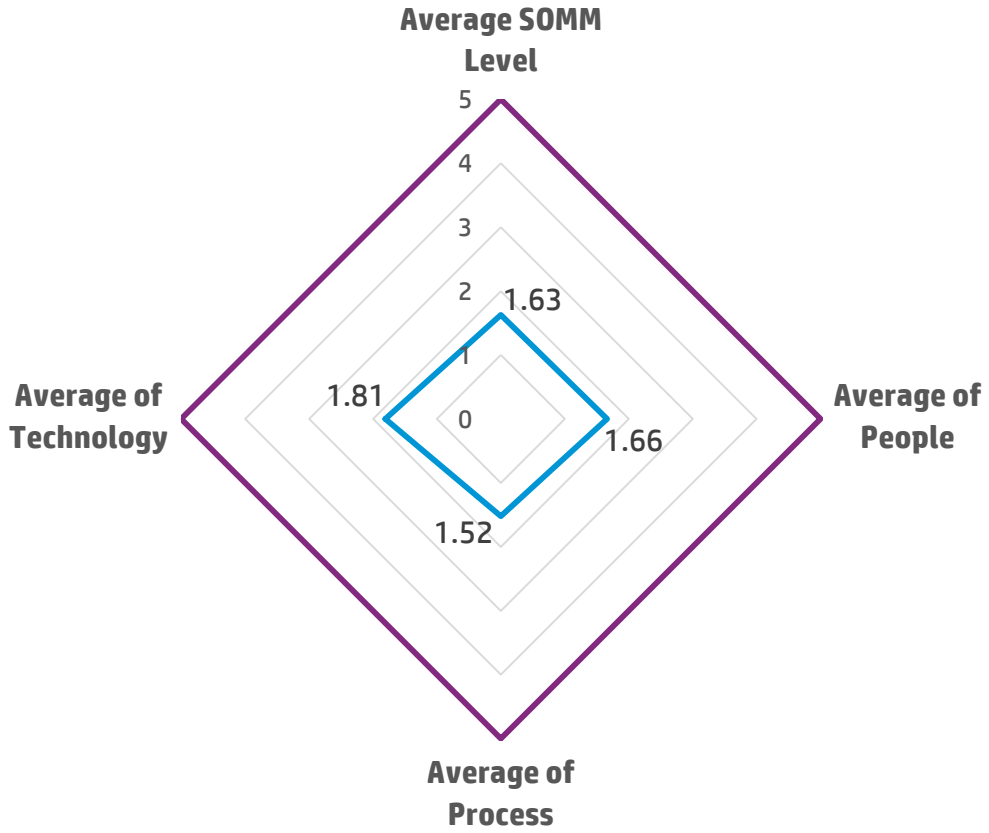
Phased SOC Strategy

	Current	Phase 1	Phase 2	Phase 3
Timeline		6 mos	1 yr	2 yr
SOMM Target	1.6	2.0	2.5	3.0
Use Cases	Logging	Perimeter, compliance	Insider Threat, APT	Application Monitoring
Staffing	Ad hoc	4 x L1, 1x L2	8 x L1, 2x L2	12 x L1, 2x L2, 2x L3
Coverage	8x5	8x5	12x7	24x7

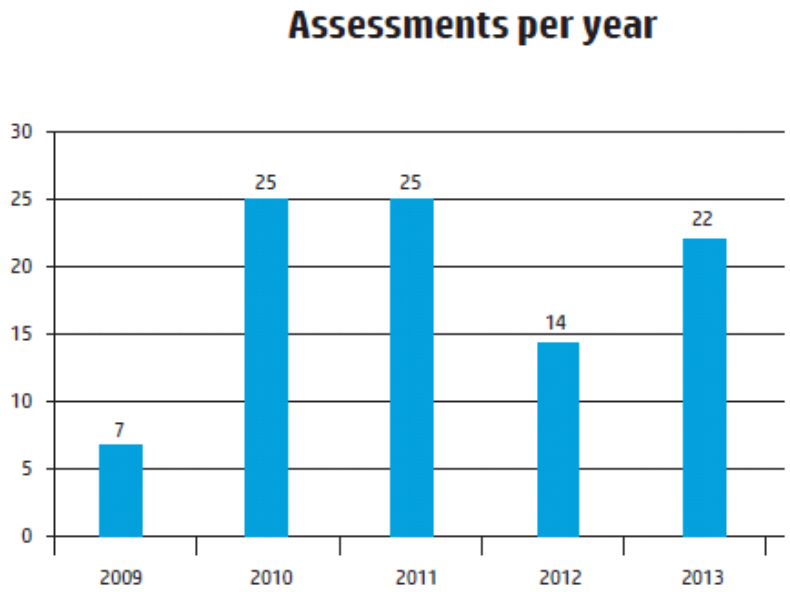
Capability & maturity baseline

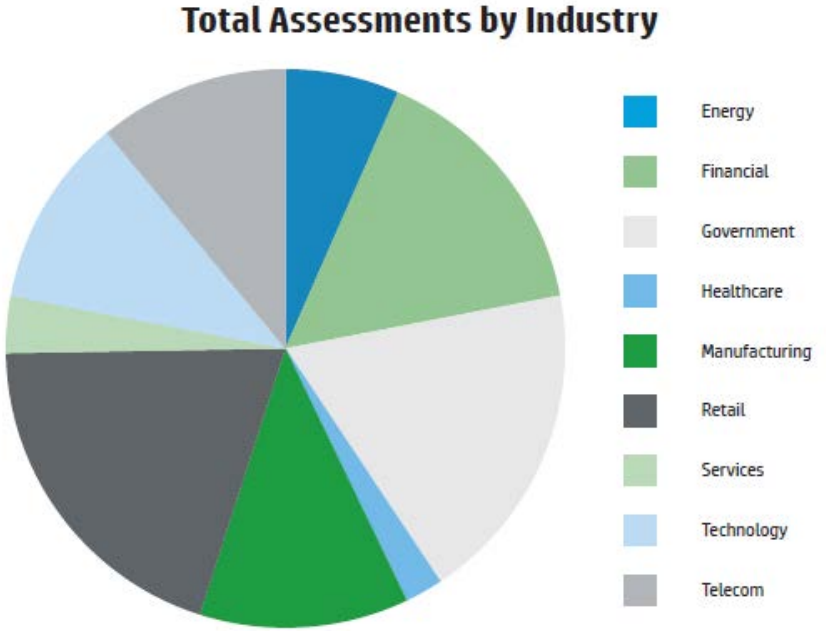
Maturity Assessment	Score	Comments
Business	**2.44**	
Mission	1.86	
Accountability	1.21	
Sponsorship	2.18	
Relationship	2.15	
Deliverables	3.00	
Vendor Engagement	2.67	
Facilities	1.27	
People	**1.82**	
General	1.98	
Training	2.61	
Certifications	1.58	
Experience	2.00	
Skill Assessments	0.88	
Career Path	1.92	
Leadership	1.50	
Process	**0.63**	
General	2.01	
Operational Process	1.67	
Analytical Process	0.00	
Business Process	0.00	
Technology Process	0.00	
Technology	**2.60**	
Architecture	1.54	
Data Collection	3.69	
Monitoring	1.50	
Correlation	1.37	
General	2.13	
Overall SOMM Level	**1.69**	

Totals through November 2013

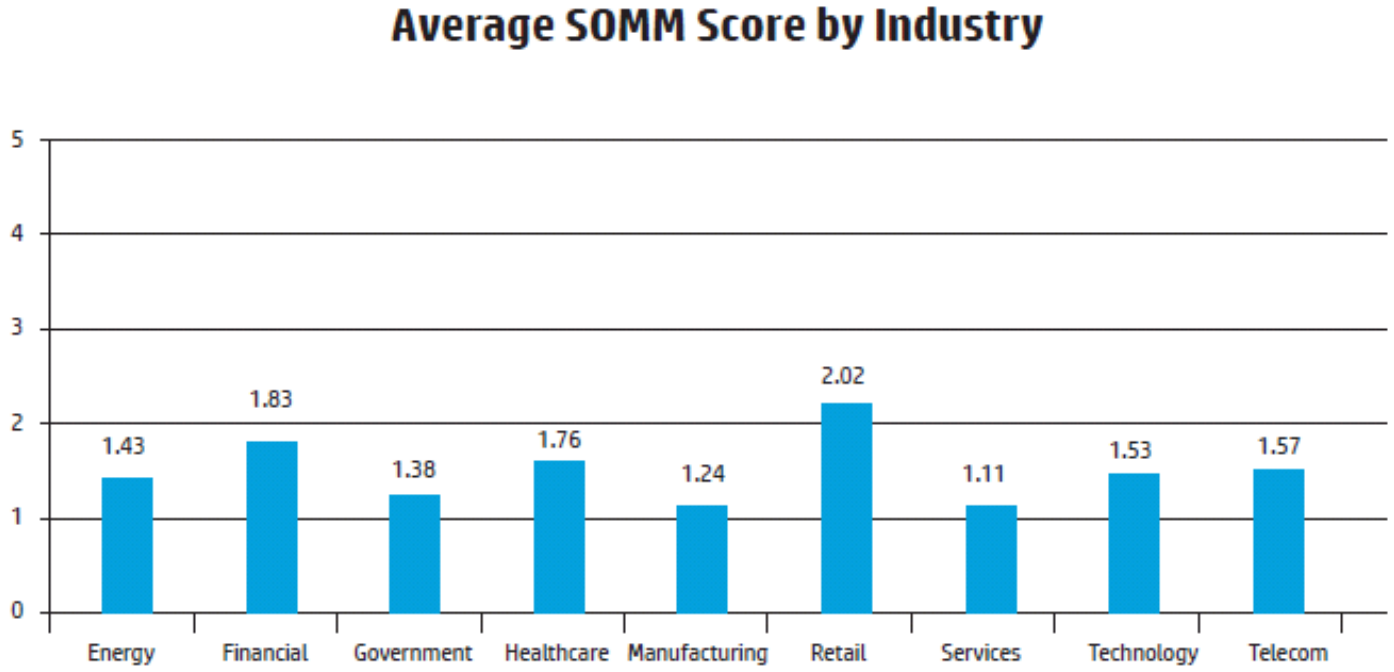


Totals through November 2013

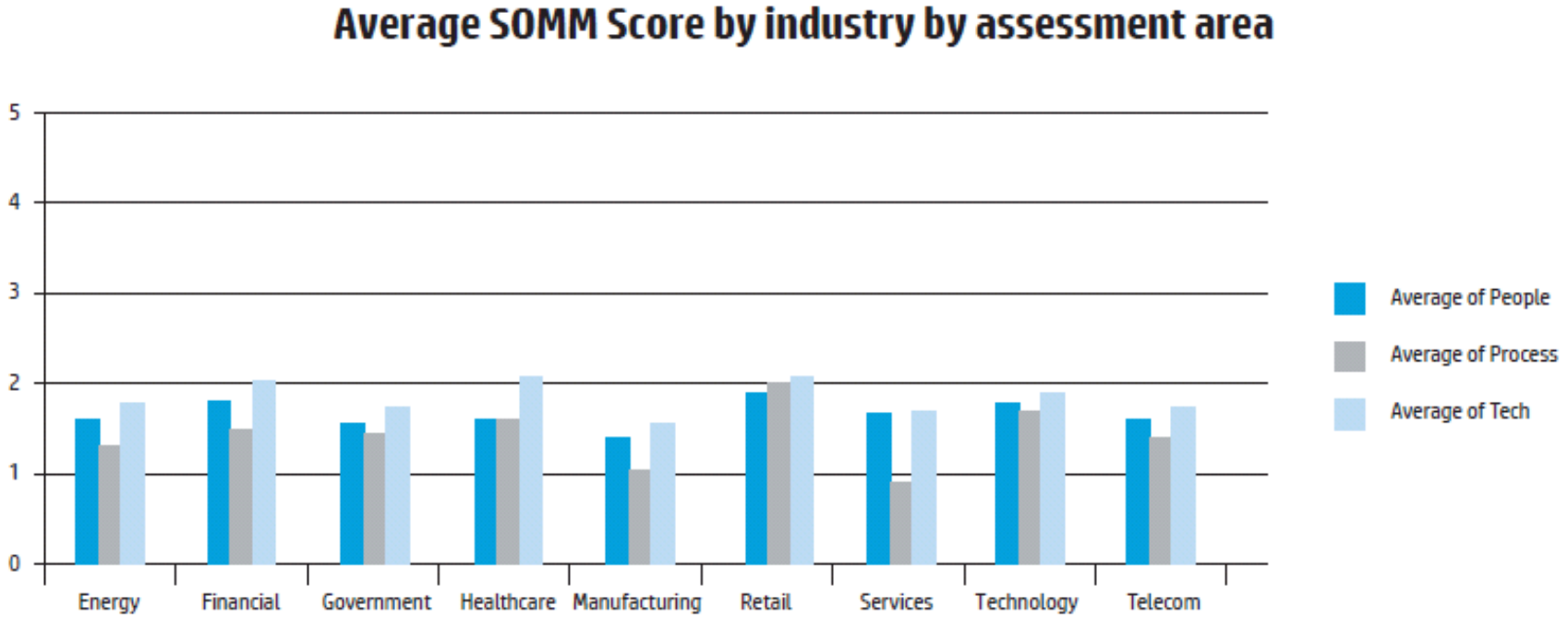




Totals through November 2013



Totals through November 2013



Challenge #1: Lack of organizational support

SOCs do not operate in a vacuum

SOCs **must** interact with every part of the organization they are monitoring & protecting

Without an executive sponsor and support of the SOC's mission from the entire organization, a SOC will be ineffective

Challenge #2: Over reliance on technology

Organizations often spend most of their security budget on technology. This results in improperly staffed/skilled operations teams

Staffing the proper skills is required to achieve the goals of the organization

Human analytical capability is required to detect and respond to modern threats

Challenge #3: Basics are overlooked

The basics of IT security are extremely important and commonly overlooked – Asset management, user ID administration, information classification and vulnerability management

Centralization and correlation of these data feeds in a SIEM is essential for basic capabilities of a security organization

Challenge #4: Focus on compliance

Compliance does not equal security

Compliance is a side effect of a highly capable threat detection function; effective detection does not result from compliance alone

Challenge #5: Set it and forget it

Organizations often spend a lot of resources building up a security operations capability but focus crumbs after the first goals are achieved

Continuity of focus must continue as a SOC ages in order to ensure effectiveness over time

Challenge #6: Inability to prioritize

It is difficult and costly to protect everything

A successful SOC requires clear priorities determined by a **risk-based** approach

For more information

Attend these sessions

- Tuesday, 5:00 pm, BB3055 5G/SOC: How the world's most advanced SOCs are leading the way
- Wednesday, 5:10 pm, BB3269 Analysts assemble! Tips for successful security analyst recruitment, assessment, and retention
- Thursday, 10:00 am, PN3268 Beyond real-time: Finding advanced threats with advanced analytics

Visit these demos

- DEMO3546 – HP Security Operations Center
- DEMO301 – Hunting Cyber Criminals
- DEMO302 – Succeed with SIEM

After the event

- Contact your sales rep
- HP Security Intel & Ops Consulting: http://hp.com/go/sioc
- Report: hp.com/go/StateOfSecOps
- Blog: hp.com/go/securityproductsblog
- SOC Maturity Assessment Solution brief: http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA4-4144ENW&cc=us&lc=en

Please give me your feedback

Session BB3260 **Speaker** Roberto Sandoval

Please fill out a survey.

Hand it to the door monitor on your way out.

Thank you for providing your feedback, which helps us enhance content for future events.

Thank you

Make it matter.