OpenSAMM at HP

Mike Craigue

OpenSAMM Dublin 2015

OWASP

The Open Web Application Security Project

Abstract

OWASP
The Open Web Application Security Project

HP uses OpenSAMM to prioritize new investments in secure development. HP's Product Security group has developed an innovative SAMM Self Assessment Tool to adapt the OpenSAMM process into a portable ASP.Net MVC Razor application.

It seeks to simplify the measurement of an organization's software maturity against OpenSAMM framework, help in the construction of a roadmap, and, track the progress vis-à-vis the roadmap. The tool will be available following the internal legal review.

Mike Craigue will share HP's rationale behind the development of this tool, its capabilities, and will brag a bit about the contributors behind this offering.

Views on OpenSAMM-1

OWASP
The Open Web Application Security Project

CJ Coppersmith, CTO – HP Enterprise Group

"HP's overall strategy is to continuously evolve our assurances and best practices so that our products are developed in facilities and environments that are physically and logically secure, our development methodologies assure secure design, construction and completion of highly secure products that we present to a world class secure manufacturing and delivery supply chain ecosystem.

We find standards such as OTTP-S, BSIMM and OpenSAMM to be useful in measuring our ongoing progress. We often find a need to tune these standards and metrics to the needs of R&D product development concerns, vs. the security needs and assurances for broader concerns, such as banks or insurance companies. We need metrics that are crisply measurable, operational (do you do this or not?), and actionable (what do I need to do now), as opposed to broad surveys to measure security knowledge or attitudes."

Views on OpenSAMM-2

OWASP
The Open Web Application Security Project

Timothy Youngblood, CISO – Kimberly-Clark

“We are starting down the journey of the framework and leveraging it as holistic method to drive secure code practices for internal development teams and external development standards.”

Views on OpenSAMM-3

OWASP
The Open Web Application Security Project

Phil Agcaoili, SVP & CISO – Elavon (a U.S. Bancorp Subsidiary)

“I'm a big proponent of open industry security standards and encourage others to support efforts such as OpenSAMM that seeks to improve industry adoption of reasonable security practices and that advances our understanding of why technology fails in our hyper connected world.”

The journey behind this tool

OWASP
The Open Web Application Security Project

- HP had a mature SDL in many areas, but growing in others
- Absence of a standard, comparative assessment across HP
- Pilot of manual data collection was well-received
- Partnered with our HP Enterprise Services organization to automate and centralize OpenSAMM assessment tool
- Automated tool is ready for next annual round of data collection

Tool features

OWASP
The Open Web Application Security Project

What makes HP's OpenSAMM tool unique?

- Takes a few minutes for a team to record responses
- Web interface simplifies simultaneous data collection
- Immediate comparison versus company targets or industry benchmarks
- Extensible and easy to use
- Domain-aware; makes account management easy

The team behind the tool

OWASP
The Open Web Application Security Project

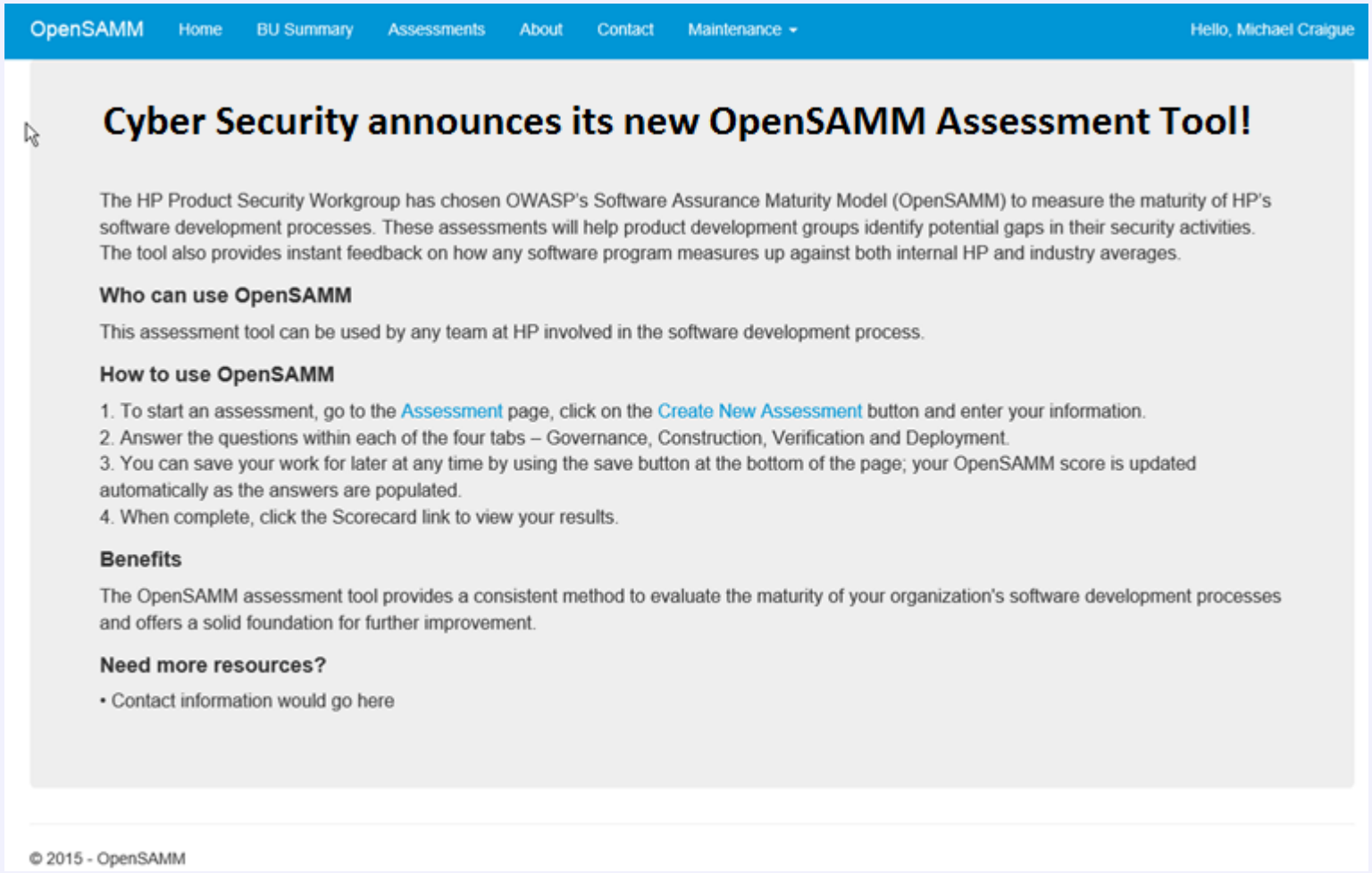
Technical Lead: **Steve Hojnacki** (HP Product Security)

Project Lead: **Mike Landeck** (HP Product Security)

Project Sponsor: **Khash Kiani** (HP Product Security)

OWASP
The Open Web Application Security Project

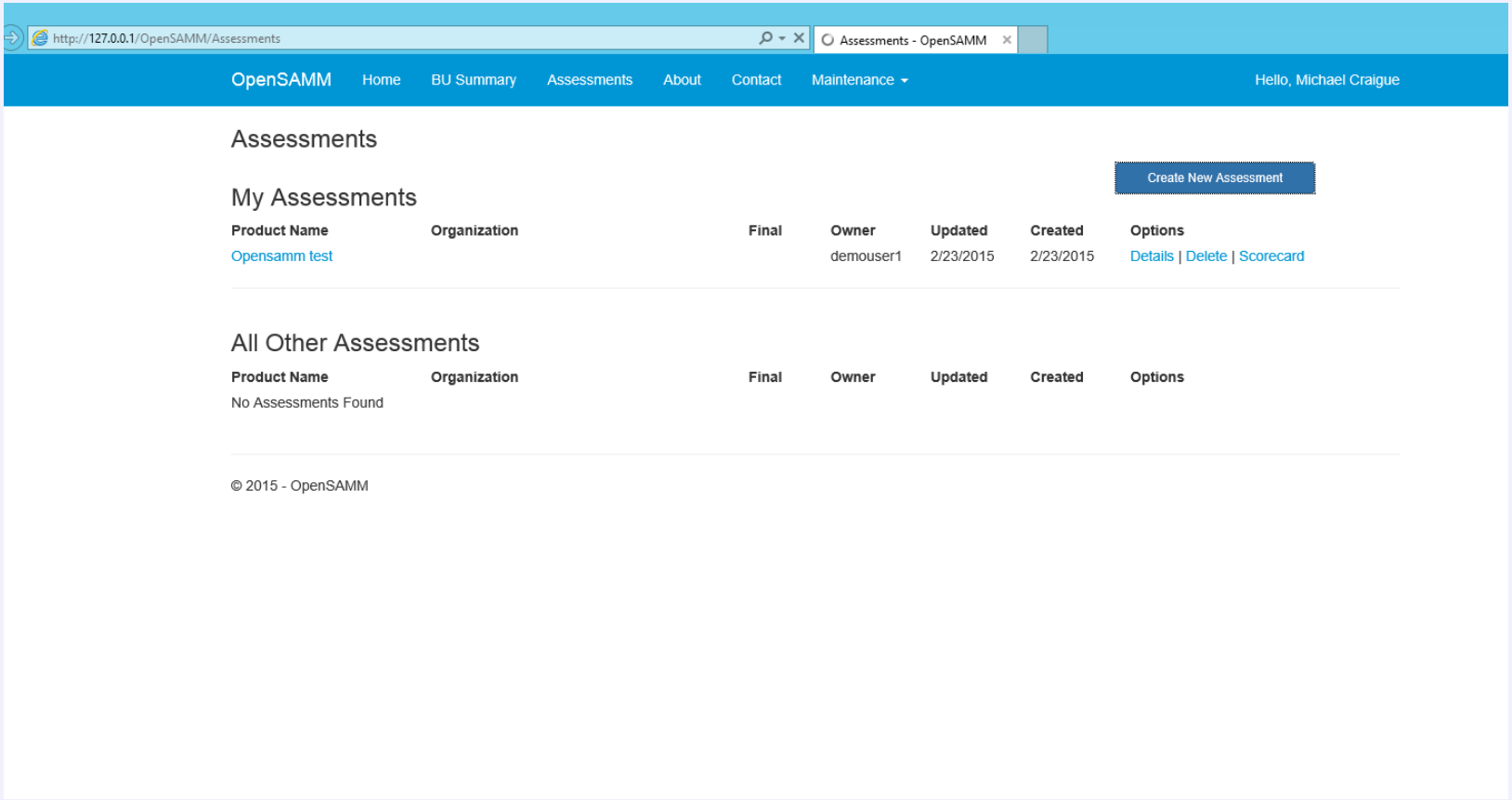
HP OpenSAMM tool demo-1



Tool Demo-2

OWASP
The Open Web Application Security Project

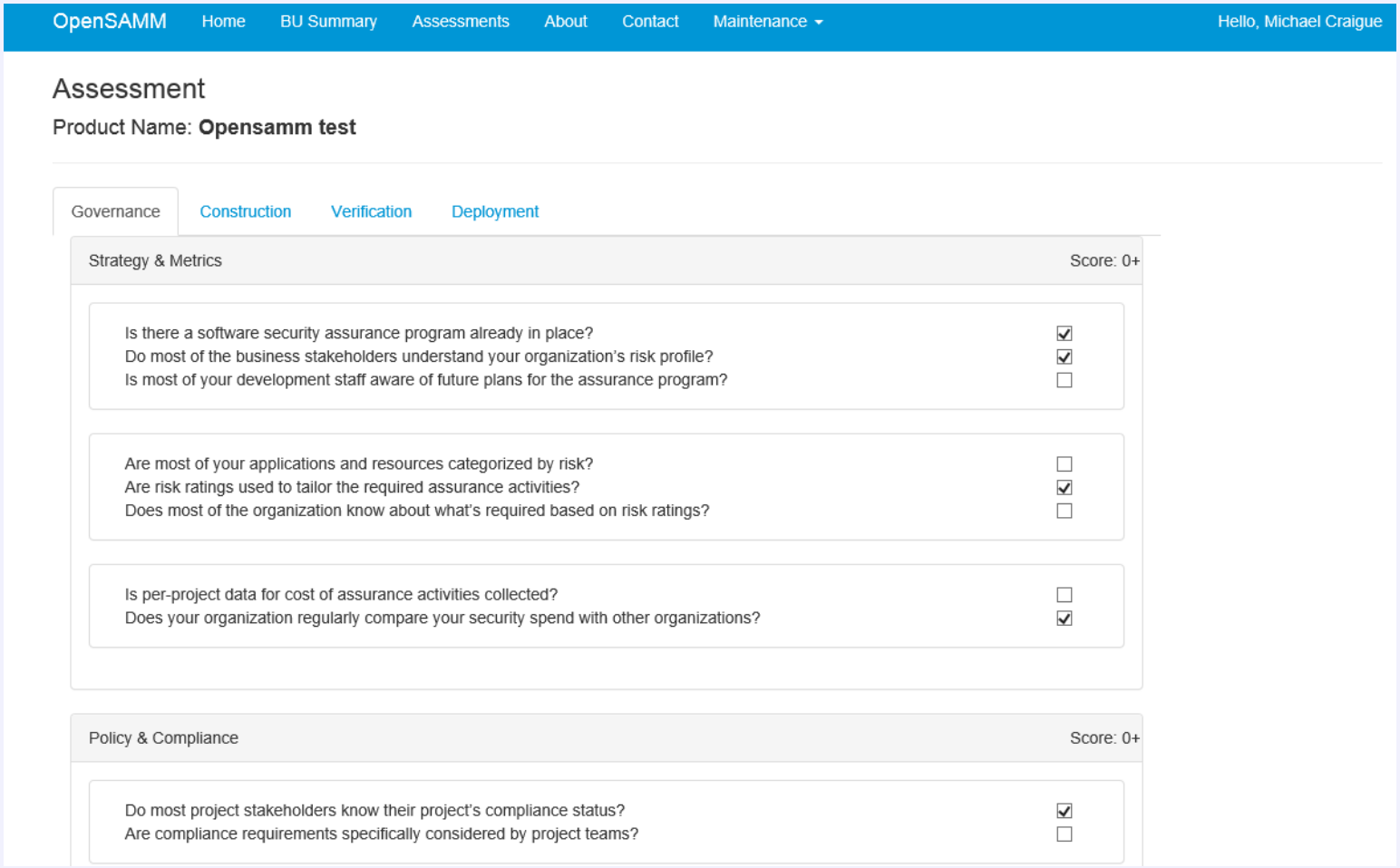
HP OpenSAMM tool demo-2



Tool Demo-3

OWASP
The Open Web Application Security Project

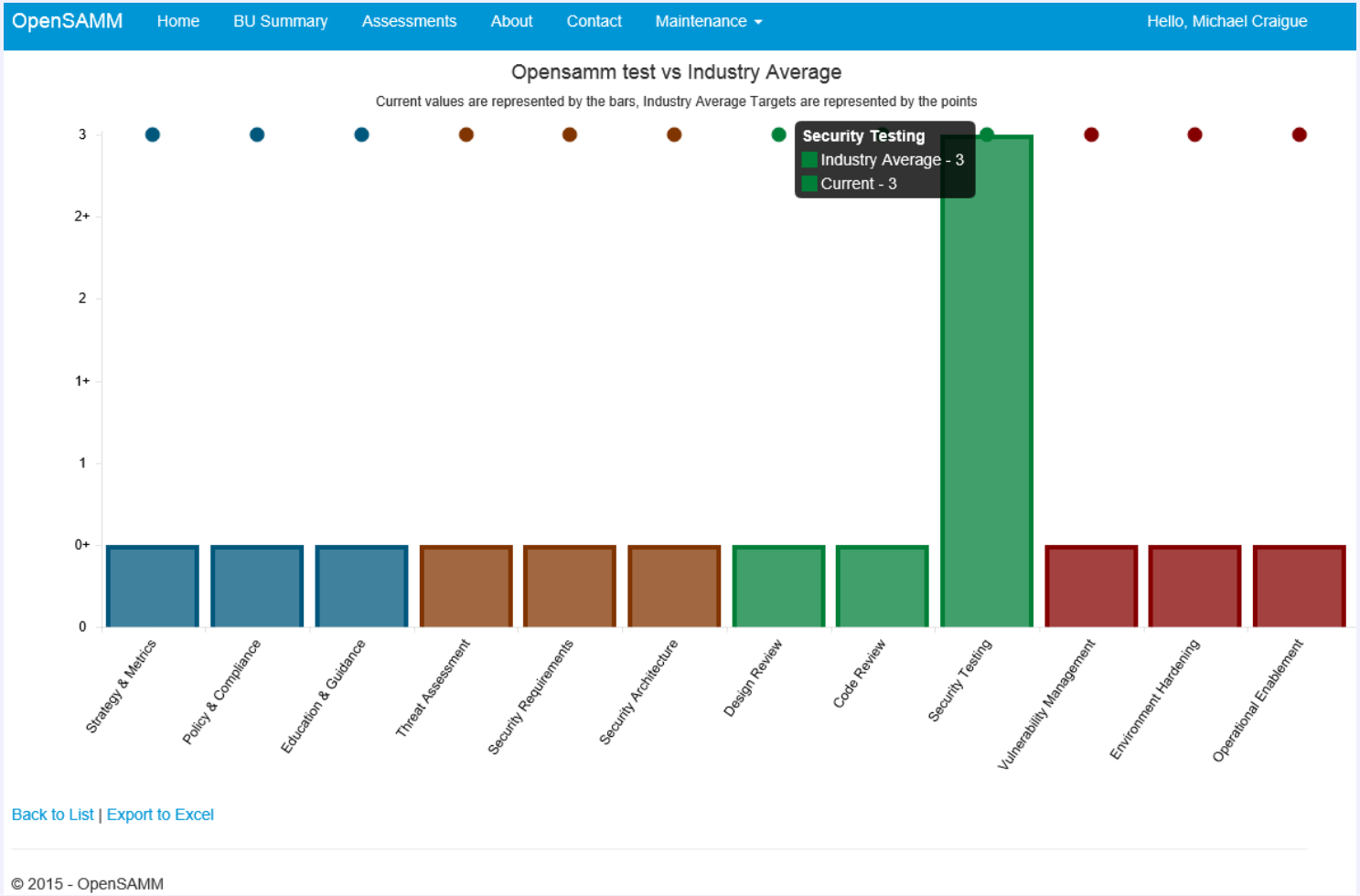
HP OpenSAMM tool demo-3



Tool Demo-4

OWASP
The Open Web Application Security Project

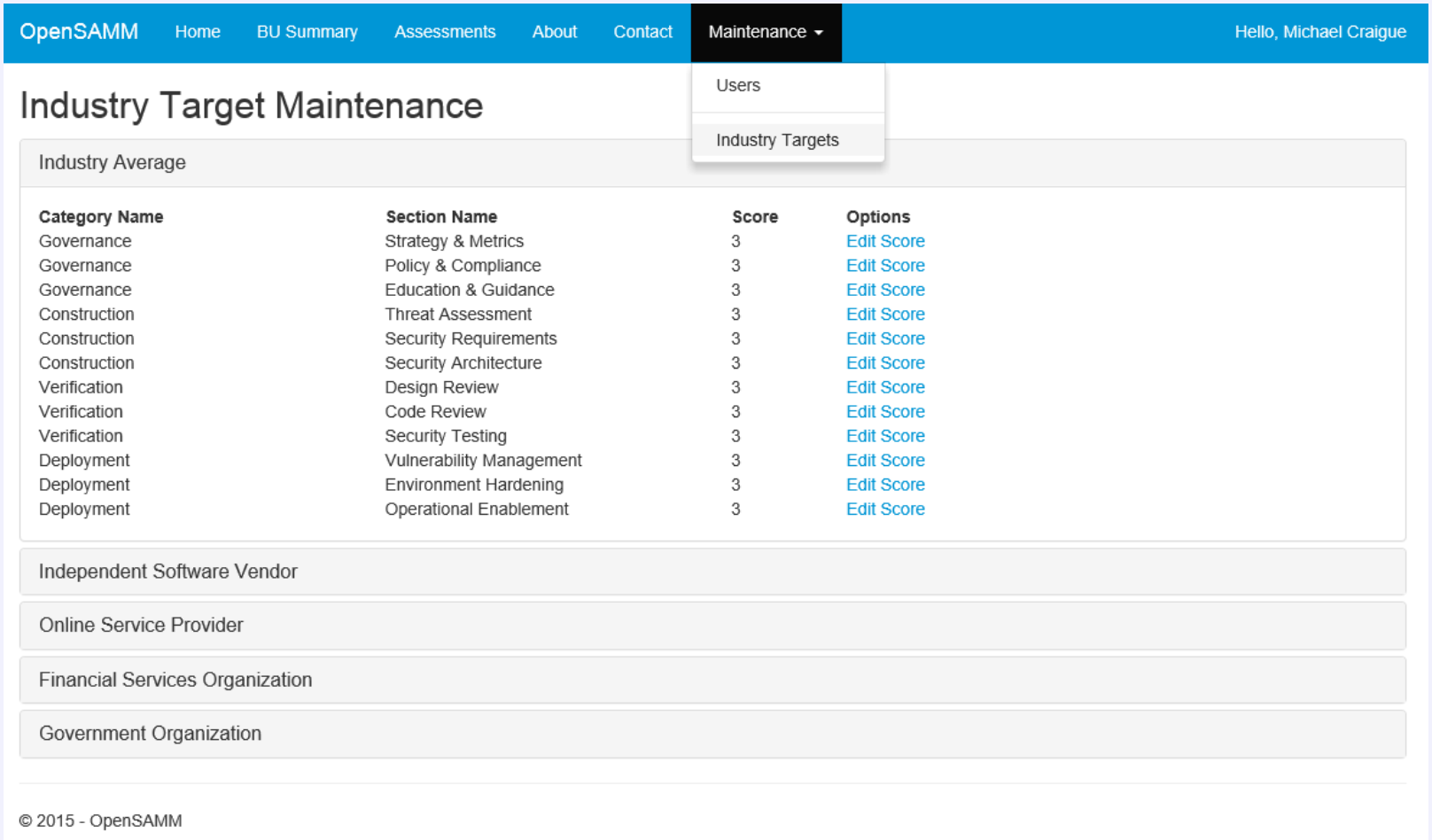
HP OpenSAMM tool demo-4



Tool Demo-5

OWASP
The Open Web Application Security Project

HP OpenSAMM tool demo-6



Next steps and roadmap

OWASP
The Open Web Application Security Project

- Gather feedback from this group
- Evaluate remediation inputs in the scoring analysis
- Weigh version 1.1 changes and possible refactoring
- Legal review for release of the tool/code to the public

OWASP
The Open Web Application Security Project

HP's OpenSAMM tool Live Demo

Additional resources

OWASP
The Open Web Application Security Project

- https://www.owasp.org/index.php/Category:Software_Assurance_Maturity_Model
- http://www.opensamm.org/
- http://bsimm.com/online/
- http://www.microsoft.com/security/sdl/discover/default.aspx

Mike Craigue bio

OWASP
The Open Web Application Security Project

Mike Craigue is the Information Security Officer in HP Cyber Security, responsible for innovative security solutions to meet growing business demands of HP Software business group.

Before joining HP in 2013, Mike worked at Dell for 14 years, most recently as the Director of Security Consulting and Portfolio Governance. Prior to Dell, he developed Web and database applications in finance and higher ed for 10 years.

Mike is an accomplished speaker and has presented at OWASP and RSA conferences in London, Stockholm, Washington, DC, and Porto Alegre, Brazil on software security, information security policy development and professional development. He has contributed to the Cloud Security Alliance's Controls Matrix project. He has also taught Database Management and Business Intelligence/Knowledge Management for MBA and MS – CIS programs at St. Edward's University, in Austin, Texas.

Mike earned a PhD from the University of Texas at Austin in Higher Education Administration & Finance, MA and BA degrees from University of Dallas. He holds CISSP and CSSLP certifications. When not at work, he enjoys cycling, cooking, and learning to play the cello.

Questions?

OWASP
The Open Web Application Security Project

Q&A