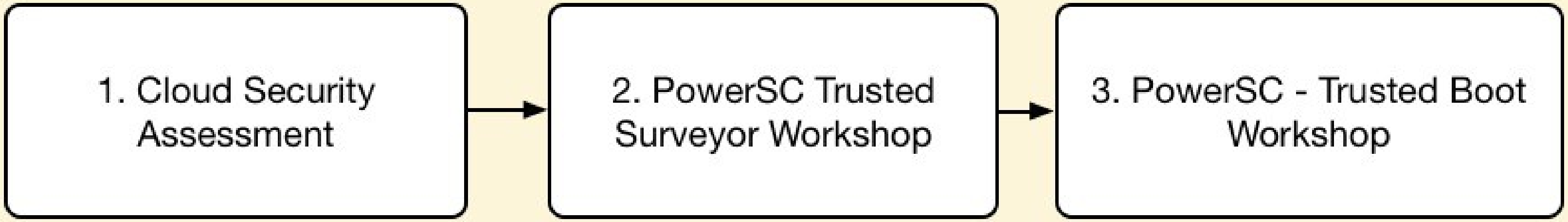
Cloud Security Services Roadmap



1. Cloud Security Assessment

2. PowerSC Trusted Surveyor Workshop

3. PowerSC - Trusted Boot Workshop

Please Note: The following roadmap is only a general suggested ordering for AIX Security services provided by IBM Lab Services. Services may be requested in any order or combination. The general ordering indicated here is based upon multiple factors such as: ease of adoption, technical considerations, functional relationships between technologies, integration considerations, etc.

AD HOC:
Integration Assistance

Created by: Stephen Dominguez - sdoming@us.ibm.com - www.securitysteve.net

Cloud Security Assessment

Overview:

Companies frequently and unknowingly can employ weak security practices that are exposing their company to high risk. The ramifications of a security breach could be unforeseeable litigation, identity theft, the bringing down of networks, and harm to a company's brand. As described by the Jericho Forum, a company shouldn't solely depend on perimeter security for their security. The Cloud Security Assessment is the best way to identify weak security practices that may be exposing your Cloud and or Cloud tenants to high risk. This assessment is a comprehensive assessment of how you are implementing security.

- One VIOS and HMC is assessed
- OPTIONAL: you may request an AIX Security Assessment to be done in combination with this assessment
- A set of documents detail the results of the assessment
- Learn about security solutions available to assist you with security & compliance
- This assessment is relevant to all Cloud service and deployment models. Its primary focus is VIOS and HMC security.
- The assessment only reads existing security settings --- not a single setting is altered in the customer environment

WHO benefits from this assessment and WHY?

- Customers wanting to improve their Cloud security configuration
- Customers wanting to stay abreast of the latest Cloud security features for Power
- Clients wanting to learn about ways to deploy their environment using recommended virtualization security practices

Duration

- At least 1 day on-site

Phase 1 – Preparation (remote):

Conference calls are held prior to the service to validate the scope, agenda, schedule and required materials.

- Client provides overview of their current Cloud Security environment
- IBM team prepares the service agenda/schedule
- IBM team details security data collection process
- IBM team provides customer security questionnaire
- Identify required materials / Finalize key players

Phase 2 – Cloud Security Assessment (on-site):

Review the Results of the Assessment with Customer

Example Tasks

- Consultant reviews the results of the security assessment with customer staff
- Customer reserves conference room with projector and invites relevant staff
- Customer staff can ask questions about the details of the assessment
- Customer staff can ask questions about the security recommendations
- Additional presentations can be provided to expound upon various technologies that may be recommended

Deliverables – Detailed Cloud Security Assessment Findings document, Heat Map, and Executive Summary

References:
The Jericho Forum:
http://en.wikipedia.org/wiki/Jericho_Forum

Terms and Conditions: Actual Tasks, Deliverables, Service Estimates,,and travel requirements vary with each client's environment. When we have reached a final agreement on the scope of your initiative and our level of assistance, a formal document describing our proposed work effort, costs, etc, will be presented for your approval and signature.

Erin M. Hansen - *PowerCare Opportunity Manager* erinh@us.ibm.com
Linda Hoben – *Opportunity Manager* hoben@us.ibm.com 1-720-395-0556
Stephen Brandenburg – *Opportunity Manager* sbranden@us.ibm.com 1-301-240-2182

PowerSC – Trusted Surveyor Workshop

Overview:

Customers sometimes feel like they are “Flying Blind” when it comes to their cloud or virtual Data Center configurations. Where are my virtual systems? Are they secure and isolated? Configuration management of a large PowerVM Cloud or virtual Data Center (vDC) can sometimes be overwhelming.

IBM has a solution to these challenges called PowerSC - Trusted Surveyor (TS). Trusted Surveyor is an AIX-based appliance partition that can register any number of HMCs. Once registered, TS uses the HMCs to survey the entire virtual PowerVM environment. When an HMC is registered with TS, a probe is created in TS that allows it to securely determine the configuration of the managed machines managed by that HMC. The configurations consist of, but are not limited to, physical frames, partitions on a frame, and their VLAN ids. This survey is called a snapshot. The snapshot is a mapping of the virtual data center configuration at a specific point in time. A snapshot can be set as a base configuration policy for the data center. Later snapshots can be compared against this policy to measure and track configuration drift that has occurred in the data center over time. Reports can be generated from snapshots to simplify and drastically expedite compliance and audit related reporting. And finally, a conveniently formatted csv file can be generated from a snapshot which can be used to do custom data mining.

- Security Zones or Groups may be defined such as: Prod, DMZ, Test, Dev etc.
- Provides an overall view of isolation (VLAN) and interconnectivity of the vDC
- Take a snapshot and compare the current configuration to previous snapshots
- Generate text and csv reporting for audits
- Creates a downloadable and formatted csv file of vDC configuration
- Many options for filtering your view of vDC configuration data
- Reduces operational expense by simplifying vDC configuration management

Duration

- 1-2 days on-site

Who Benefits from this workshop and WHY?:

- Customers wanting to meet PCI v3 network segmentation requirements
- Customers wanting to ensure the network isolation of their multi-tenant Cloud
- Customers wanting to quickly and easily learn how to use TS
- Customers wanting a solution to verify vDC configuration and isolation policy compliance
- Customers wanting a PoC installation of TS in a sandbox environment before deploying TS to their production environment

Phase 1 – Preparation (remote):

Conference calls are held prior to the service to validate the scope, agenda, schedule and required materials.

- Client provides overview of their current AIX environment
- IBM team prepares the service agenda/schedule
- Identify required materials / Finalize key players

Phase 2 – Trusted Surveyor Workshop (on-site):

Installation and configuration of Trusted Surveyor

Example Tasks

- Learn how to install and configure TS
- Learn how to configure HMC probes used by TS to walk the vDC
- Learn how TS can be used to analyze vDC configuration and set baseline policy
- Learn how to leverage downloadable csv files for custom data mining

Deliverables – Step-by-step TS install & configuration documents, TS presentation slides

Trusted Surveyor Demo

Example tasks

- At conclusion of the service, provide customer staff a demo of TS
- Provide a general Q&A session

Terms and Conditions: Actual Tasks, Deliverables, Service Estimates,,and travel requirements vary with each client’s environment. When we have reached a final agreement on the scope of your initiative and our level of assistance, a formal document describing our proposed work effort, costs, etc, will be presented for your approval and signature.

Erin M. Hansen - PowerCare Opportunity Manager erinh@us.ibm.com
Linda Hoben – *Opportunity Manager* hoben@us.ibm.com 1-720-395-0556
Stephen Brandenburg – *Opportunity Manager* sbranden@us.ibm.com 1-301-240-

PowerSC – Trusted Boot Workshop

Overview:

Having a third party host your production capabilities or confidential data can lead to fears of service disruption, data loss or a leak of sensitive information. Who's to say a cloud provider hasn't provisioned its customers with instrumented virtual machines to spy on their confidential data! having your hardware, data and network traffic overseen by a third party can create risk to your organization..

Based on the Trusted Computing Group's Trusted Platform Module (TPM) technology, Trusted Boot scrutinizes every step of the boot process, taking secure measurements (cryptographic hashes) of the software and recording them in a virtual TPM (VTPM).

Trusted Boot forms an unbreakable chain of trust for every step of the boot process. For Power Systems, this chain starts at the hypervisor, continues through the partition firmware and into AIX and the application layer. Each link in the chain is responsible for measuring the next and locking this measurement away in the VTPM where it cannot be tampered with. For AIX, this means that before it has had a chance to execute a single instruction of its own code, it has been pulled apart, placed under the microscope and had the measurements locked away where it can't touch them. If anyone has modified the boot image on disk, Trusted Boot will know.

WHO benefits from this workshop and WHY?

- Customers with limited or no experience with Trusted Boot
- Customers wanting to properly configure Trusted Boot
- Customers wanting to evaluate Trusted Boot before deploying it to their production environment
- Customers wanting to meet security compliance requirements, such as PCI v3

Duration

- 1-2 days on-site

Phase 1 – Preparation (remote):

•Conference calls are held prior to the service to validate the scope, agenda, schedule and required materials.

- IBM team prepares the service agenda/schedule
- Identify required materials / Finalize key players

Phase 2 – Trusted Boot Workshop (on-site):

Installation and configuration of TFW

Example Tasks

- Learn how to install and configure Trusted Boot
- Learn how to troubleshoot Trusted Boot

Deliverables – Step-by-step Trusted Boot install and configuration documents,

TFW Demo

Example tasks

- At conclusion of the service, provide customer staff a demo of TFW
- Provide a general Q&A session

References:

http://www.ibmsystemsmag.com/aix/administrator/security/trusted_boot/

Terms and Conditions: Actual Tasks, Deliverables, Service Estimates, and travel requirements vary with each client's environment. When we have reached a final agreement on the scope of your initiative and our level of assistance, a formal document describing our proposed work effort, costs, etc, will be presented for your approval and signature.

Erin M. Hansen - *PowerCare Opportunity Manager* erinh@us.ibm.com
Linda Hoben – *Opportunity Manager* hoben@us.ibm.com 1-720-395-0556
Stephen Brandenburg – *Opportunity Manager* sbranden@us.ibm.com 1-301-240-2182

Integration Assistance

Overview:

Our standard services provide our customers with the essential knowledge transfer and Proof of Concept deployment to enable them to take the next steps from Proof of Concept to Production. The Integration Assistance service is a purely optional service that provides additional assistance to help customers more quickly and easily take that next step from Proof of Concept to Production.

This service is a general technical service that can be requested solely or combined with one or any number of our standard services to assist customers with the deployment of any AIX security related feature to your production environments. For example, 3 weeks of deployment assistance can be added to the one week RBAC workshop in order to assist you with integrating RBAC into your production environment.

This service can also be requested for general technical security assistance with the implementation of any arbitrary security solution. In this type of assistance, we only provide our best effort to assist, since we are providing assistance with possibly a solution with which we might have no prior experience. However, our assistance can greatly expedite and increase the chance of successful implementation since you will be leveraging a highly experienced security technical resource.

Service Highlights:

- Obtain general technical assistance with deploying AIX security related functionality into your production environments
- Can be requested with any of our standard services
- Technical services are provided with whatever combination of local/remote support desired
- Ensure you are deploying security features according to best practice
- Expedite the integration of security features by leveraging a Lab Services consultant who can also leverage an AIX development network

WHO benefits from this service and WHY?

Our workshop services are typically done in a sandbox environment for proof of concept purposes. After you have had a chance to evaluate and learn about the new technology in our workshop service, you may request this service to help you deploy the technology to your production environments.

Duration

1 or more weeks on-site/remote technical assistance

Phase 1 – Preparation (remote):

Conference calls are held prior to the service to validate the scope, agenda, schedule and required materials.

- Client provides overview of their current AIX Security environment
- IBM team prepares the service agenda/schedule
- Identify required materials / Finalize key players

Phase 2 – Security Integration (on-site/remote):

Example Tasks

- Consultant reviews implementation process
- Customer provides guidance with implementing security functionality
- Consultant can resolve complex technical issues leveraging the IBM development network
- Consultant verifies methodology used for integrating security tooling is consistent with best practices
- Consultant provides implementation guidance based upon previous customer environment deployments

Terms and Conditions: Actual Tasks, Deliverables, Service Estimates,,and travel requirements vary with each client's environment. When we have reached a final agreement on the scope of your initiative and our level of assistance, a formal document describing our proposed work effort, costs, etc, will be presented for your approval and signature.

Erin M. Hansen - *PowerCare Opportunity Manager* erinh@us.ibm.com
Linda Hoben – *Opportunity Manager* hoben@us.ibm.com 1-720-395-0556
Stephen Brandenburg – *Opportunity Manager* sbranden@us.ibm.com 1-301-240-2182