Information Management FORUM

FORUM INFORMATION

IT Security Summit 2015

June 15 - 16, 2015
Annapolis, Maryland

- ♦ **Low/No-Cost Security Best Practices**

- ♦ **Re-Architecting for Network Security**

- ♦ **Fraud Detection Through Data Analysis**

- ♦ **Ethical Decision-Making and Leadership**

About The IMF

The IMF is the best source of unbiased information in IT. Since 1975, we have remained unique as a vendor-free, enterprise-wide membership for IT executives to share best practices and ideas. Our members are industry leaders who favor intellectual discussion over packaged opinions and diverse backgrounds over geographic or industry specific groups. We provide the highest quality personal service for a group of select members and work to be the best value in their IT budget.

IMF Meetings

ITFM Meetings are vendor-free events that promote an open exchange of ideas across all aspects of IT Finance. They provide excellent opportunities for developing your professional network while hearing real best practices from industry peers. Why are these meetings valuable?

⇒ Build **lasting relationships** with colleagues across member organizations nationwide.

⇒ **Vendor-free environment** promotes transparent dialogue amongst attendees.

⇒ Hear **real best practices, strategies, challenges, and management techniques** from your peers.

⇒ Opportunities for presentation before senior IT Finance executives in **Fortune 500 companies**.

⇒ Specific topics of interest at ITFM Meetings are **determined by ITFM member organizations** versus analysts or vendors.

Three Easy Ways to Register

Web: theimf.com/IMF-Events.htm   **Email:** registration@theimf.com

Phone: 770.455.0070

Agenda

Day One: Monday, June 15

8:15   Breakfast

9:00   Company Introductions

10:00 Break

10:15 Presentation: Re-Architecting for Network Security
          Speaker: Paul Kincaid, IT Security Architect, VMware

As networks grow more and more complex, attacks increase in sophistication. And with the proliferation of virtualization in datacenters, the ability for a Security Operations Center (SOC) to effectively monitor attacks is significantly more difficult than it was even five years ago. This discussion will center around two solutions for this growing complexity (micro-segmentation) and the increase in attack sophistication ('The Goldilocks Zone'). Micro-segmentation is the technique of applying firewalls on the individual interfaces of systems or virtual machines for finer grain control of traffic into and out of a system or VM. "The Goldilocks Zone" is the concept that monitoring either on the host itself or via the network each have their weaknesses - "The Goldilocks Zone" is the concept of getting the best of both worlds by monitoring host-based attributes and the network traffic, both via the hypervisor.

11:15 Presentation: Fraud Detection Through Data Analysis
          Speakers: Jeff Banks and Michael Willette, USAA

USAA, a longtime leader in big data analytics, uses the capabilities of big data to assist in fraud detection as a world-class financial services company. Learn from USAA's tried-and-true methods to evaluate how big data can work for your organization's plan to detect and prevent fraud.

12:15 Lunch

1:15   Presentation: Busting the Hackers, Not Your Budget
          Speaker: Sheryl Hanchar, Director of Information Security, Broadcom Corporation

Broadcom Corporation is a global leader and innovator in semiconductor solutions for wired and wireless communications, managing one of the industry's broadest portfolios of state-of-the-art system-on-a-chip and embedded software solutions. Broadcom developed leading-edge technology to identify and minimize intrusion attempts. Hear innovative and inexpensive ways to identify attackers and limit vulnerability at your organization.

Agenda

Day One: Monday, June 15 (cont'd.)

2:15   Break

2:30   Presentation: The U.S. Senate's Strategic IT Security Plan
Speaker: Paul Grabow, Chief Information Security Officer, United States Senate, Sergeant at Arms

The U.S. Senate faces vulnerability to cyber attacks both foreign and domestic. Mr. Grabow developed a comprehensive plan to strategically evaluate threats and develop security measures to defend against them. He will share successes, failures and lessons learned, allowing attendees to better identify their own vulnerabilities and evaluate their security plans.

3:30   Facilitated Discussion on Topics from the Day

4:15   Adjourn

6:00   Dinner

Agenda

Day Two: Tuesday, June 16

8:15   Breakfast

**9:00   Presentation: Leadership Discussion—Ethical Decision-Making and Leadership
Speaker: Captain James Campbell USN (Ret.), Distinguished Military Professor, U.S. Naval Academy**

Captain James Campbell, a U.S. Naval Academy instructor, will lead a leadership discussion on ethical decision-making as a core component of organizational leadership. The presentation will feature case studies as a basis for an interactive discussion.

10:15 Break

**10:15 Presentation: The FBI on Cyber Crime
Speaker: TBD**

The FBI leads the national effort to investigate high-tech crime, including cyber-based terrorism, espionage, computer intrusions and major cyber fraud. To stay in front of current and emerging trends, the FBI gathers and shares information and intelligence with public and private sector partners foreign and domestic. A member of the FBI will brief attendees on the current state of cyber crime.

11:15 Future Meeting Planning

12:00 Adjourn