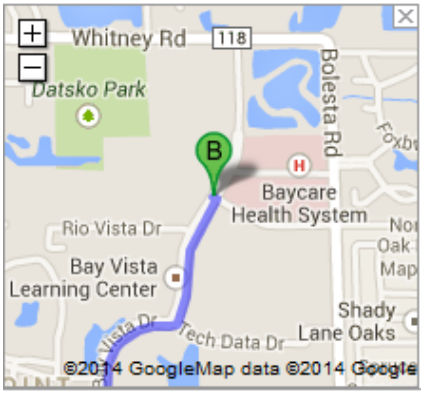
Tampa Bay ISSA February 20th Meeting Agenda

@ Techdata - 16202 Bay Vista Drive Clearwater, FL 33760 (**MAP & DIRECTIONS**)



8:30-9:00 - Breakfast and Networking

9:00-9:45 – Daniel Ingevaldson, Easy Solutions

Title: Target and Neiman Marcus Breach - Insight, Early Warning and the Black Market

Abstract: The Target and Nieman Marcus breaches bring to the fore once again the challenges that all retailers and financial institutions face to maintain control of cardholder information and to contain breach associated costs. In this talk, we'll examine some of the root cases, show the size and structure of the black markets fueling these breaches and discuss lessons learned.

Speaker Bio: Not available.

10:00-10:45 – David Hobbs, Radware

Title: DDoS Mitigation Tactics

Abstract: Not available.

Speaker Bio: David Hobbs has two decades of security experience. David has worked as a consultant to many federal agencies ranging from the FBI, US Army Counterintelligence, Secret Service and many private investigation companies. David worked for Washington Mutual Bank as well as Fishnet Security. David has worked in many security practices from exploit research, penetration testing, forensic investigation, security countermeasures, wireless and radio security, social engineering, and compliance.

During his time at Fishnet Security, David developed and taught ethical hacking classes as well as showing how systems are vulnerable and the many ways to exploit them. David consulted many of Fishnet Security's customers daily in regards to their security needs.

David has worked with most of the major security technologies and vendor products. David has worked with most of the various firewalls, IPS/IDS, UTM, Malware Prevention, encryption technologies, and security service providers. David's vast knowledge has allowed him to work effectively in most customer environments.

11:00 – 11:45 – Scott De Lelys, Palo Alto

Title: The Dynamic Threat Landscape and Next Generation Security

Abstract: Network attacks are becoming both more sophisticated and more common, with all types of enterprises and all types of information being targeted by attackers. In this presentation, we will shine light on the lifecycle of a modern network attack to understand how the threat landscape has changed and what is required from us as security professionals to protect our networks and users today.

Speaker Bio: With over 12 years in the field of information security, Scott has hands-on experience with Firewalls, Virtual Private Networks, Intrusion Detection/Prevention Systems, Vulnerability Scanning Systems, Email and Web security solutions. Trained as an Ethical Hacker, Scott has performed a number of security assessments for small commercial companies as well as large enterprise organizations and government entities. He maintains the CISSP certification and a number of security vendor certifications. Prior to joining Palo Alto Networks, Scott worked as a security engineer for Cisco, IBM, Internet Security Systems and security consulting firms in Florida.

12:00-1:00 - Lunch and Networking

1:00 – 1:45 – Chris Beier, Trusteer

Title: Latest Fraud and Risk Trends and Mitigations

Abstract: Malware continue to present significant problems to enterprises and is a leading factor to nearly all data breeches. Effectiveness is an indicator of the success of any security technologies. Unfortunately, traditional technologies have lost their effectiveness to stop or prevent advanced threats. New approaches are needed. In this presentation Christopher Beier from Trusteer, an IBM Security company will present the new age of security technologies in the context of how attack materialize in the enterprise. Attacks have a specific life cycle and anatomy that when studied present strategic phases where new technologies can be deployed to detect, preempt, and prevent attacks. You will learn:

- The phases advanced malware traverses during the attack
- The types of security technologies and their effectiveness during each phase
- The pros and cons of each type of technology

Speaker Bio: Christopher Beier is a Senior Product Marketing Manager for Trusteer. Trusteer has recently been acquired by IBM and is part of IBM Security. Christopher brings significant security DNA through his almost 20 years' experience working for companies like Symantec, and McAfee. Christopher has deep knowledge and experience in the financial services and online banking security space through is 5 years with Fiserv. He is also a 12 year US Navy veteran where he applied IT administration skills to the US submarine corp.

2:00 – 2:45 – Steve Lowing, Promisec

Title: Advanced configuration and host management

Abstract: To secure against cyber-attacks, organizations must vigorously defend their networks and systems from a variety of internal and external threats. To aid in this effort, the SANS Institute publishes and updates 20 Critical Controls for Effective Cyber Defense. The goal of the Critical Controls is to help organizations develop a defensive posture to protect their critical assets, infrastructure, and information through continuous, automated protection and monitoring of their IT infrastructure.

This talk explores the top 5 Critical Controls and identifies best practices for IT and security personnel when implementing automated solutions to assure that every endpoint on the network is properly protected and in compliance with established security policies.

Speaker Bio: Steve is Director of Product Management at Promisec, a pioneer in endpoint visibility and remediation software that empowers organizations to avoid threats and disarm attacks that can lead to unwanted headlines and losses. Prior to Promisec,

Steve has held similar product roles at Core Security, Symantec and EMC. Steve has a Bachelor's of Science in Computer Science and started his career designing and developing software including development of two security solutions.

3:00 – 3:45 – Joe Partlow & Michael Rogers

Title: Intro to Memory Forensics

Abstract: This talk will discuss latest techniques and tactics used in Memory Forensics and well as an introductory walk-through on how to get started.

Speaker Bio: Joe Partlow has been involved with InfoSec in some capacity or role for over 15 years, mostly on the defensive side, but always fascinated by those cool kids on offense. Current projects include mobile and memory forensics, SIEM optimization, disaster recovery and business continuity planning. He is currently the Chief Information Security Officer at ReliaQuest, a local information security professional services company.

Michael Rogers is an Information Technology Security Engineer with ReliaQuest. He enjoys capture the flag competitions, computer forensics, cyber security and StarCraft. He is currently pursuing his Masters of Science Degree in Cyber Security at Florida Institute of Technology.