Thursday, September 26, 2013

8:00 am - 9:00 am **Registration and Networking Breakfast**

9:00 am - 9:15 am **Opening Remarks**
Bob Bragdon, Publisher, CSO magazine

9:15 am - 10:00 am **A Change in Perspective: Enterprise Security in the Age of Adaptive Persistent Threat**
John Burke, CIO & Principal Research Analyst, Nemertes Research

The nature of today's attacks is changing. Low and slow is the battle call as sophisticated attackers bombard our networks and blow through traditional defenses that worked well not so long ago. While new technologies are making their way into the battle lines -- including those that focus on packet data inspection and exfiltration monitoring -- less than 15% of businesses are actually using them. Has the time come to make a wholesale shift in how we think about and defend the enterprise? Join us as we explore the current and future state.

10:00 am - 10:30 am **Building APT Protection with Data-Centric Security**
Sol Cates, Chief Security Officer, Vormetric

A key enabler to APT is privileged accounts that are compromised. This fundamental flaw in distributed systems gives attackers access to data they should never see. And while monitoring and detection are critical steps to avoidance, preventing privileged user access from being used against your organization should be the highest priority. Despite our best intentions, however, traditional perimeter security is failing. In the aftermath of a breach, most organizations don't even know they were targeted. Their security solutions simply failed them. And 94% of the time, the breaches were reported by third parties -- and firewalls, network and perimeter security defenses didn’t catch them. Simply put, the APT tornado is growing, gathering speed, and — like it or not — we're all in its path. So what can you do to prevent your organization from losing this battle? Join Vormetric’s Alan Kessler as he discusses how attackers get through conventional safeguards every day, and how you can protect your company’s sensitive data.

Presented by Vormetric

10:30 am - 11:00 am **Networking Break**

11:00 am - 11:30 am **Five Implementation Principles for a Global Information Security Strategy**
Mike Towers, VP, Information Security Assurance, GlaxoSmithKline

Many large corporations with significant dependency on intellectual property and personally identifiable information are struggling with protecting their data. Improvements in attacker proficiency, increasing numbers of analytics systems storing sensitive data, and continually evolving risks with cloud computing, mobility and outsourcing make defense capabilities difficult to build and maintain. Information security leaders must apply both their expertise and influence wisely: identifying and targeting the high priority areas with maximum business impact, and invoking the necessary implementation resources and tools. Join us as we discuss the five critical success factors CISOs should explore and apply to their own enterprise.

11:30 am - 12:15 pm **Managing Security Incidents: Making Sense Through All the Noise**
John Burke, CIO & Principal Research Analyst, Nemertes Research
Craig Shumard, CISO Emeritus, Cigna; Principal, Shumard and Associates
Dr. Andrei Stoica, Director, Global Information Assurance, IMS Health
Bob Bragdon, Publisher, CSO magazine

Simply put, security and technology teams need to see what's happening to their enterprises in real-time. As enterprises have introduced more defensive and monitoring technologies to their infrastructure, making sense out of all the resulting data is daunting -- but no longer a luxury, it's a necessity. Technologies like SEIM can be critical to making quick sense of data while attacks are still under way. But making all of this work to your best advantage isn't always simple. Join us to learn the best strategies for making sense through all the noise.

12:15 pm - 1:30 pm **Networking Lunch**

Join a table to share strategies and connect with your peers to hear how they're resolving the same issues with which you grapple every day.

1:30 pm - 2:00 pm **Cyber Security Confab Sessions**
Kirk Appelman, SVP, Global Sales, CounterTack
Ashley Stephenson, Chief Executive Officer, Corero

Join us for this lightning round of 15-minute, rapid-fire presentations designed to inform and educate on a variety of Mobile Security challenges and solutions.

Presented by CounterTack

How to Get Enterprise-Wide Visibility of Advanced Threat Behavior

The cyber security landscape has changed for enterprise organizations. APTs have advanced to the point where even innovative, well-constructed security models fall short in keeping attackers out of business-critical systems. As a result, sophisticated attackers continue their path of destruction. They evade network-based detection platforms and disable host technologies like antivirus software. All of this leaves organizations with no visibility of how long attackers have controlled desktop and server endpoints. But there are solutions. Join us to find out how you can get enterprise-wide visibility of advanced threat behavior in real-time, thereby significantly reducing attacker 'dwell-time' -- the amount of time an attacker remains inside any system. All of this allows you to combat threats in real-time and counter targeted, persistent threats to your business.

Presented by Corero

DDoS in the Enterprise: Defending Against an Evolving Threat Landscape

If your organization relies on the Internet to conduct business, you are automatically a potential target of a Distributed Denial-of-Service (DDoS) attack. When carried out, DDoS attacks -- volumetric and application layer — have the ability to not only create a business outage, but also compromise confidential information. Join us for this session to learn why traditional technologies, including firewalls, aren't enough to protect you against DDoS — and understand the strategies you need to put into place to more completely defend against DDoS.

2:00 pm - 2:30 pm

Creating an Effective Insider Threat Program: The Challenges and Opportunities

Michael Theis, Chief Counterintelligence Expert, CERT Insider Threat Center

Why do you need an Insider Threat Program as part of your cybersecurity strategy? How do you convince senior leadership of that, and what are the truly essential components of an effective program? This empirically based strategy will ensure your program framework meets the needs of your organization. Join us to see how your organization can Prevent, Detect, and Respond to insider threats in ways that meet your needs as well as those of privacy, governance and compliance.

2:30 pm - 3:30 pm

What to Do -- and Not to Do -- When Attacked: A Moderated Workshop

Nick Akerman, Partner, Dorsey & Whitney LLP

Bob Bragdon, Publisher, CSO magazine

Today’s enterprises have more powerful security resources than a decade ago. Some have been tempted to turn those resources against their attackers in retaliation for the damage they caused. Others are reluctant to work with law enforcement on investigations for fear of exposing a negative incident to the public. In this session, we’ll learn more about what every business should do -- and not do -- when responding to cyber attacks.

3:30 pm **Recap, Takeaways and Closing Remarks**
Bob Bragdon, Publisher, CSO magazine