Protecting America's Energy through Cybersecurity

7th Annual API Cybersecurity Conference for the Oil and Natural Gas Industry

November 13-14, 2012
Westin Houston Memorial City
945 North Gessner Road
Houston, TX

Event check-in: Pick up your badge or register onsite on the 4th Floor.

On-Site Meeting Agenda

Day One – Cybersecurity Conference – Tuesday, November 13, 2012

Day One	Sessions
7:00 – 8:00 AM	**Continental Breakfast – *Sponsored by Ernst & Young***
8:00 – 8:10 AM	**Welcome Opening Remarks and Safety Moment** David Zacher, Marathon Oil and Jessica Garrison, Shell, Conference Co-Chairs
8:10 – 9:10 AM	**Session K1: KEYNOTE – STATE OF OIL & GAS THREATS** **Industrial Control Systems: Applications to Enhance Community Security** 2012 has been a fast paced year in the world of ICS security. Mr. Cornelius will discuss a few key events and the salient takeaways from them. He will also help identify ways these lessons learned can be applied across the ICS domain to enhance the security posture of the community as a whole. **Speaker: Eric Cornelius, Chief Technical Analyst, Control Systems Security Program/Industrial Control Systems-Cyber Emergency Response Team** **Moderator: David Zacher, Marathon Oil**
9:15 – 10:10 AM	**Session K2: -- ADVANCED PERSISTENT THREATS / NEXT GENERATION / ADVANCED EVASIVE TECHNIQUES** **Anatomy of a Targeted Intrusion** Whether you're reading today's media headlines or receiving alerts from your perimeter network defenses, you're flooded with news of this and that malware breach. Many take comfort in the solace afforded by these alerts - if a threat has a name, then there's undoubtedly protection against it. While a lot of security teams associate these alerting mechanisms with the termination of a threat, all too many find that reassurance to be ill founded. This session will discuss the specifics of how an espionage professional will engage and navigate your industrial networks once access has been purchased from an everyday malware attack. We'll discuss how these professionals navigate the network undetected, leave false trails and employ non-malware tools that ensure thy can both retain perpetual access to the network and leapfrog to other networks as they choose. In essence, we'll discuss the anatomy of a modern targeted intrusion and the organizations that support them. **Speaker: Gunter Ollman, VP Research, Damballa** **Moderators: Curt Craig, Hunt Consolidated and Paul Huttenhoff, Phillips66**
10:10 – 10:30 AM	**Morning Refreshment Break - *Sponsored by Fidelis Security Systems***

10:30 – 12:00 PM	***Track A – Azalea 1&2*** **Session A1: APPLICATION SECURITY** **A1 A: Implementation Patterns for Software Security Programs** While there are a number of components of software security programs that are reasonably standard, there are different ways of implementing tools and deploying processes so what was successful for one organization does not guarantee success in others. This presentation is based on experiences working with several organizations creating software security programs and relates several example case studies for organizations rolling out different portions of their software security programs. Three specific software security activities will be discussed: static code analysis, dynamic application testing and developer security education. **Speaker: John Dickson, Principal, and Dan Cornell, CTO & Principal, Denim Group** **A1 B: Hacking Databases: Exploiting the top vulnerabilities and misconfigurations** According to the Identity Theft Resource Center, in the past year and a half, there have been close to 900 breaches and over 28,000,000 records compromised. With groups like Anonymous and LulzSec continuously hacking into major corporations and government agencies, do you wonder if you're next? No organization, industry, or government agency is immune to the proliferation of complex attacks and malicious behavior. Ensuring database security is a priority for organizations interested in protecting sensitive data and passing audits. Over the course of this presentation, a description of some of the sophisticated methods used in invading enterprise databases will be discussed, and the evolution of the security issues and features in each will be provided. A demonstration of popular attacks will also be presented. The presentation will conclude by proposing essential steps IT managers can take to securely configure, maintain databases, and defend against malicious breaches entirely. Attendees will leave with a basic understanding of the most effective methods for protecting their data, an enterprise's most prized asset, from attackers today and in the future. Attendees will: (1) Learn how organizations, through an integrated defense strategy, can effectively manage their database risks across large, heterogeneous database environments with automated controls; (2) Understand the common vulnerabilities and misconfigurations used to attack databases; and (3) Methodologies and best practices on how to implement actionable plans to protect enterprise database assets. **Speaker: Josh Shaul, CTO, Application Security, Inc.** **Moderator: David Zacher, Marathon Oil**	***Track B – Azalea 3*** **Session B1: INFORMATION PROTECTION TECHNOLOGIES / DRM / DLP** **B1 A: The Case for "Reverse Information Classification** One of the basic tenets of information security is that information must be classified to determine which controls should be applied to appropriately secure the data. While this philosophy may have worked in the "paper world", there is sufficient empirical and anecdotal evidence that using classification to select controls does not work well in the "electronic world". Rather than continue down the formal classification path and expect different results (Einstein's definition of insanity), perhaps we should try something different, reversing the process and using controls to select the classification. This "reverse information classification" focuses attention on the controls which actually protect the information while maintaining original classification concepts. **Speaker: Michael J. Lewis, Senior Staff Security Strategist, Chevron** **B1 B: Using Data Loss Prevention (DLP) Solutions to Protect Critical Assets and Intellectual Property** This session will provide an in-depth view into how organizations across the globe are leveraging Data Loss Prevention solutions to protect intellectual property and other sensitive data elements. Business Process and Technical Speaker Rob Eggebrecht will bring experience from 400+ DLP projects that span numerous industries and vast geographic coverage to provide the audience with invaluable knowledge transfer. The presentation will include case studies on successful DLP program designs and best practices including application management, policy governance, incident triage, event management and business analytics. **Speaker: Robert Eggebrecht, President & CEO, BEW Global** **B1 C: How I "Pwn" Your Network: A Chat with a Social Engineer and Industrial Spy** Do you want to know what hackers and spies are doing to your infrastructure? Would you like to see how we are able to evade your expensive physical security and gain access to your valuable intellectual property? Stop wondering and ask! In this highly interactive and demonstration rich session, you'll chat with a professional social engineer and facility breach expert, as he discusses what works and what doesn't in protecting the "trade secrets" that gives you a competitive advantage. You'll hear what makes his job harder....and sometimes easier. Don't miss this rare engagement! **Speaker: Kai Axford, Director of Strategic Services, FishNet Security** **Moderator: Mark Freed, FMC Technologies, Inc.**
12:00 – 1:00 PM	**Attendee Lunch in Azalea 4 – *Sponsored by McAfee***	

1:00 – 2:10 PM	**Session A2: OPERATIONAL TECHNOLOGY / PCS/ICS/SCADA SECURITY** **Rethinking SCADA Security: Are Current "Best Practices" Missing the Mark?** In 2008, the Industrial Control Systems community was shaken, as the first public SCADA exploit was released. What followed was the opening of "Pandora's Box" as Stuxnet, and subsequent variants, emerged, 34 0-Day ICS vulnerabilities were released, and "Project Basecamp" exposed a plethora of ICS vulnerabilities, just to name a few. Although cyber security awareness and vigilance in the industrial sectors has grown over the past few years, we are still behind the curve. Asset owners and operators find their resources stretched thin as they struggle to keep up with the sheer number of threats, balance security with productivity, and try to maintain compliance with standards and regulatory requirements. Unfortunately, the very "best practices" that are currently recommended and being deployed may be fundamentally flawed. Is there a better way? Can organizations efficiently secure their systems and maintain compliance without risk to operations or over extending resources? Utilizing statistical data on industrial vulnerabilities and incidents over the past decade, this presentation examines SCADA threats and vulnerabilities at their source. It offers a more efficient, proactive, and pragmatic approach to security by gaining a better understanding of the threats, instead of reacting to each individual vulnerability alert and deploying blanket best practices. **Speaker: Clint Bodungen, Security Analyst, Amor Group** **Moderators: Curt Craig, Hunt Consolidated & Rebecca Renner, Marathon Oil**	**Session B2: INCIDENT RESPONSE MANAGEMENT** **B2 A: Measuring an Organization's Response Program** Effectively responding to a security incident is heavily dependent upon your organization's monitoring capabilities, the maturity of the response process, the skill level of the individuals charged with this responsibility, and the technologies that facilitate the investigation of potential incidents. Unfortunately, having an immature security monitoring program may lead to a lack of incident detection and introduce delays in the response process. Furthermore, the response program itself must be measurable through a series of metrics that not only identify how effective the program is operating today, but also offer some insight into threat intelligence through tracking of attacker actions, objectives, and process. In this presentation, KPMG will provide an overview of security monitoring and response program maturity levels and what it takes to get to "the next level", moving detection closer to the attack and providing valuable insight during the response. Case studies from response efforts will be used to highlight the failures in security monitoring and incident response that we have witnessed over the past year. The presentation will conclude with a discussion on how to measure the effectiveness of a response program through key performance indicators and how to classify events in terms of attacker capability and motivation by tracking key risk indicators of incidents. **Speaker: Deron L. Grzetich, KPMG** **B2 B: System State Intelligence Before, During and After an Incident** Because organizations have invested heavily in SEIM they expect a measurable return on that investment in the form of greater security and lower risk. Unfortunately SEIM only detects an incident, informing those organizations exactly when security is lessened and risks are increased. System state intelligence (SSI) compliments the SEIM, before, during and after a breach by informing the organization of potential risks, providing timely situational awareness, and the showing the context in which an incident occurred. The objective of this session will be to provide valuable information on proactively improving an organization's risk posture by combining SEIM and SSI, how to use SSI during an incident, and finally how this information informs the business. The intended audience will be managers, directors, security and compliance officers and anyone who has struggled with proving the value of their SEIM investment. **Speaker: Jim Wachhaus, Principal Consultant, TRIPWIRE** **Moderator: Dee Michael, Shell**
2:10 – 2:20 PM	**Transition Break**	

2:20 – 3:20 PM	**Session A3: CLOUD COMPUTING** **Enterprise Class Identity-as-a-Service for Employees, Partners, Customers** As enterprises adopt cloud, embrace mobility and engage online with partners and customers, they are encountering a new wave of identity management challenges that legacy identity management systems (IdM) can't address. From cloud SSO for employees to IAM for external portals, a cloud IdM service provides a secure, robust, easy to use solution. This session will cover: Internal and external IdM challenges; IdM across cloud and web apps; Integration with directories and legacy IdM; and Enterprise security and reliability requirements. **Speaker: Todd McKinnon, CEO & CoFounder, Okta** **Moderator: David Zacher, Marathon Oil**	**Session B3: CYBER THREAT INTELLIGENCE & INFORMATION SHARING** **B3 A: Threat Intelligence and Situational Awareness (Awesome! But HOW do I do this?!)** Cybersecurity has come to encompass so much more than what it once did. In the recent past, most people believed that cybersecurity was only relevant to IT Security Specialists or guys sitting in their moms' basements trying to hack into anything and everything. However, in today's world, and in the immediate future, cybersecurity is no longer relevant to the few – it applies to EVERYONE! Who are your enemies, attackers, thieves? How might they get to you, your company, your people, your data? What do they really want?! To be prepared and subsequently defend, you must gather the appropriate information that leads to useable and actionable knowledge – also known as Threat Intelligence Gathering and increasing your Situational Awareness. So, how is this done? During this session, you will learn the who, what, where, when, why, and how to build your threat intelligence gathering process. Take aways will include lists of information sources, analysis guidelines, distribution guidelines, and "further reading" recommendations to continue honing your skills and process. **Speaker: Halana Demarest, Level 2 CSMC Analyst, Shell Information Technology International** **B3 B: Security Analytics - Addressing Security's "Big Data" Problem** Information security professionals are drowning in data from the various security tools, feeds and sources they have established over the last decade. Even after spending millions on tools, even tools to manage other tools and data, most security professionals are still relying on their "gut" and experience. Although this information is useful, most organizations have a "big data" problem within security and are struggling with finding a way to effectively organize, correlate and use this data. This presentation will offer a point of view to addressing this growing problem using a technology enabled analytics framework developed by Ernst & Young. The approach leverages your existing data and tools, and is focused on enabling the security professional with the ability to make fact based decisions. Are you drowning in data? **Speakers: Anil Markose, Senior Manager, Ernst & Young National Information Security Practice** **Moderator: Dee Michael, Shell**
3:20 – 3:40 PM	**Afternoon Refreshment Break – *Sponsored by Bit9***	

3:40 – 5:00 PM	**Session K3: CIO Panel Discussions** This session provides an opportunity to hear oil and natural gas industry CIOs and CISOs share their thoughts on different aspects of executive security, both physical and cyber security, around the following themes: • Moving Beyond the Mobile Executive and E-mail: How to Securely Distribute Confidential Information to Mobile Devices • [Addressing/Listening to/Adopting to] the Voice of Consumerism • Preparing for the Data Breach: Steps to Take NOW to Help Prepare for the Inevitable • "*It is easier to hack a person than it is to hack a machine."* Social Engineering and What Are You Doing About It? • Spelling "Kloud" with a "K". Seriously? Marketing Hype Surrounding the Web-based Model **CIO Panelists:** **1. Rich Schmidt, Shell Projects & Technology** **2. Celia Lin, Chevron** **3. Trond Ellefsen, Statoil Gulf Services** **4. Thom Sneed, Marathon Oil** **Moderator: Kevin Campbell, Hunt Consolidated, Inc.**
5:00 – 6:30 PM	**Welcome Reception and Networking - *Sponsored by PhishMe***

Day Two – Cybersecurity Conference – Wednesday, November 14, 2012

Day Two	Sessions
7:00 – 8:00 AM	**Continental Breakfast – *Sponsored by RSA***
8:00 – 8:10 AM	**Opening Remarks and Safety Moment - *Curt Craig, Hunt Consolidated***
8:10 – 9:10 AM	**Session K4: KEYNOTE - EMERGING THREATS / EMERGING TECHNOLOGIES** **Protecting the Digital Oilfield in the 21st Century from Advanced Persistent Threats** Every business is a potential target for today's complex, sophisticated and increasingly frequent advanced persistent threats. The industrial control systems used by oil and natural gas companies are especially high-risk targets because of the devastation a successful attack could cause. Our utility and infrastructure systems sit on the front lines of this new cyber battlefield. Flame, Duqu, Gauss and other APTs cannot be stopped by traditional security technologies. There is no silver bullet, but trust-based application control that prevents unknown software from running at refineries, pipelines and other high-risk targets is the best defense in this escalating cyberwar. **Speaker: Harry Sverdlove, Chief Technology Officer, Bit9** **Moderator: Curt Craig, Hunt Consolidated, Inc.**
9:15 – 10:10 AM	**Session K5: CRITICAL INFRASTRUCTURE PROTECTION / ICS** **Why Are Critical Infrastructure Assets so Easy to Attack? And How Can We Protect Them?** Can a criminal entity or terrorist group -- from the other side of the world -- take out down the Internet and telecommunications systems? Or launch a worm that disrupts oil and gas pipelines, water and electric power distribution? How will America cope if the outages last for days? **Speaker: Dr. Sujeet Shenoi, University of Tulsa** **Moderator: Scott Crane, Williams**
10:10 – 10:30 AM	**Morning Refreshment Break - *Sponsored by Globalscape***

10:30 – 12:00 PM	***Track A* – *Azalea 1&2*** **Session A4: MOBILITY / MOBILE DEVICE MANAGEMENT & ALTERNATIVE MODELS "The Different Aspects of Consumerization of IT"** **A4 A: Mobile Security in the Enterprise** Provide participants with sufficient information to analyze evaluate and recommend a suitable option to manage risk associated with mobile devices within the enterprise. – Understand the drivers for mobility and mobility security considerations (corporate culture to drive solution) – Understand the mobility ecosystem – Understand the risks and various categories associated with mobility (RA) – Approach and Strategic choices for a mobile security solution deployment **Speaker: Adnan Amjad, Lead Identity Management Services Partner, Delloitte's Mid-America Region** **A4 B: Good app gone bad: Turning a helpful oil & gas app into mobile malware** Mobile risk factors and potential damage more broadly as well. The key takeaway is the concrete demonstration of mobile malware in action and its consequences. – Attack Vectors on Android and iOS platforms – Data Protection, security mechanisms, and their efficacy – Cutting-edge research into emerging mobile threats **Speaker: Ted Eull, Vice President, Technology Services, viaForensics** **A4 C: Legal Perspectives on IT Consumerization** Legal risk factors of BYOD – "Work is not a place anymore. It is a state of mind." BYOD creates significant new challenges in the following areas: (1) Companies have less control over their data when it is stored and transmitted with employee-owned devices; and (2)Employees may use their dual-use devices on personal time for activity that would be prohibited in the workplace. This program will review these data management and employment law issues and identify best practices companies can consider to mitigate the risks. **Speaker: Michael McGuire, Littler** **Moderatos**: **Catharina Budiharto, Rod Holmes & Zach Grieshop, Marathon Oil**	***Track B* – *Azalea 3*** **Session B4: EMERGING CYBER THREATS IN THE OIL & GAS SECTOR** Three important topics in the arena of cybersecurity are discussed and analyzed. Targeted techniques and new attack vectors are discussed, followed by advanced targeted attacks directed at the energy sector. Afterwards, we discuss IPV6 and the threat implications that this brings to the table, and why IPV6 should not be ignored. **B4 A: Title: You Drop the (Cyber) Bomb on Me: A Primer on Cyber Warfare Tools & Techniques** You are now witnessing the first shots fired in the first full-blown "klicks-krieg". Your perimeter is irrelevant as the threat is targeting users with advanced cyber-attacks. Cyber-espionage, stealing IP from your organization with social engineering and malware like Stuxnet and Flame, is everywhere. Cyber-warfare, the targeting of critical infrastructure and key resources with customized malware like Stuxnet, is an evolving threat. You need to be informed. Join us for this informative and engaging session in which we'll discuss and demonstrate these new attack vectors. **Speaker: Kai Axford, Director of Strategic Services, FishNet Security** **B4 B: Title: Protecting the Oil Industry from Advanced Targeted Attacks** Spear Phishing, and other advanced targeted attacks, are a top priority for the energy and utility industry. In the last six months energy and utility organizations have seen a 60% increase in incidents. As the Night Dragon attack dramatically illustrated, critical infrastructures of energy and utility companies are under attack. In this case, criminals went at intellectual property, information on ongoing exploration, and records associated with bids on oil and gas reserves. **Speaker: Alex Lanstein, Senior Engineer, FireEye** **B4 C: Title: IPv6: Security Implications, David Mehl, Principal – Security Governance and Process, Dexa Systems** The Internet is in the midst of a very fundamental change. Internet Protocol version 4 (IPv4) has been the foundation of the Internet's success since 1982. However, a newer version of Internet Protocol, version 6 (IPv6), has been released after years of testing and is now been deployed into production on the Internet. Multiple major web sites, core Internet Backbone providers, and ISPs are now supporting access by IPv6. Moreover, most new computers including Windows, Linux, and Apple all install IPv6 support out-of-the-box. While IPv6 will bring many opportunities for improved network operations and better security, most organizations will continue to use IPv4 for the foreseeable future, while IPv6 capability is being added in bits and pieces. However, organizations can no longer safely ignore IPv6. If they do, organizations face significant cyber vulnerability. **Speaker: David Mehl, Principal, Security Governance and Process, Dexa Systems** **Moderator: Ionel Chila & Ken Rivet, Chevron**
12:00 – 1:00 PM	**Attendee Lunch in Azalea 4, visit with exhibitors and networking - *Sponsored by Okta***	

1:00 – 2:10 PM	**Session A5: RISK MANAGEMENT** **A5 A: Combatting Cyber Security Issues with IT Audit and Consulting** Cyber security professionals in the energy industry are faced with the dual challenges of ever increasing security requirements and constant focus on efficiency and cost control. If your organization has an IT audit group, learn how you can leverage each other's results and resources to address specific security issues. Session Objectives: • Understanding the purpose of IT audit vs. information security • Gaining visibility to security performance via the IT audit process • Approaches for leveraging mutual interests and resources • Developing a plan to work together **Speaker: Brian J. Thomas, Partner in Advisory Services & Brittany George Teare, Manager in Advisory Services, Weaver LLP** **A5 B: Quantitative Risk Assessment (QRA) – In Theory and in Practice** Quantifying the risk associated with cyber security is important to the management of cyber security. In this paper, you will hear of the progress made in making cyber risk quantification easier to do and to understand. This has been achieved using a security management framework and a structured approach to threats, vulnerabilities and losses. Losses, in particular, are most important in framing the quantitative analysis results. An example will be used to demonstrate the results. **Speakers: Theodore van Rooy, Research Analyst & Herbert Yuan, CTO, Dexa Systems** **Moderator: Steve Kellison, Baker Hughes**	**Session B5: OPERATIONAL TECHNOLOGY / PCS/ICS/SCADA SECURITY** **Stories from the Trenches: Securing Industrial Control Systems with Application Whitelisting and Change Detection** This will be a technical discussion on how to leverage the naturally deterministic characteristics of industrial control system environments to harness the features of application whitelisting and change detection technologies to improve performance and reduce security risks. There will be a particular focus on the processes and equipment used in the oil and gas sector with experience drawn from deployments in that industry. The intended audience will be individuals responsible for protecting control systems as well as those with managerial oversight. Additionally, individuals responsible for responsible to incidents and overseeing the overall security posture would also benefit. **Speaker: Gib Sorebo, Chief Cyber Security Technologist & Vice President, SAIC** **Moderator: Curt Craig, Hunt Consolidated & Rebecca Renner, Marathon Oil**
2:10 – 2:20 PM	**Transition Break**	

2:20 – 3:20 PM	**Session A6: ENDPOINT SECURITY** **Creating a Secure Desktop** In this session, Group Policy MVP Derek Melber will go over some of the most important, yet forgotten, security settings for Windows desktops. Settings like LanManager, Anonymous, IE, UAC, etc. will be covered and you will see why these settings are so important for every corporation. You will get the information you need to not only configure these settings, but also how to audit them during your Windows audit. **Speaker: Derek Melber, President, BrainCore.Net AZ inc.** **Moderator: Rick Handley, Schlumberger**	**Session B6: CLOUD COMPUTING** **Cloud-Based Technologies for Improving Cyber-Security in Petrochemical Applications** At an increasing rate, data in large petrochemical corporations is being integrated and shared across powerful information networks that employ approaches such as service oriented architectures (SOA), semantic integration or cloud computing. These information networks provide improved means for data modeling, information retrieval/sharing, automated reasoning, and user access. These information networks require a new approach to cyber-security – based on Security Risk Assessment - to combat the increase in cyber-attacks. To provide appropriate risk assessment, next generation information security systems can be built to leverage the power of their underlying cloud-based (and semantic) technologies in three key areas: Infrastructure-Enhanced Security, Enhanced Threat Modeling and Semantic Security. **Speaker: Eric Little, Director Information Management & Steve Hamby, CTO, Orbis Technologies, Inc.** **Moderator: David Zacher, Marathon Oil**
3:20 – 3:40 PM	**Refreshment Break – *Sponsored by Fishnet Security***	
3:40 – 5:00 PM	**Session K6: SOCIAL ENGINEERING** **K6 A: Patching Layer 8 – Improving Security Awareness** Despite all of the defences thrown at protecting all layers of the network stack, attackers still compromise our networks by targeting the vulnerabilities at Layer 8 – the User layer. Much of the security awareness education seems to have very little impact. Find out why security awareness education is often done incorrectly and find out what needs to be done to increase safe behaviour from your employees. Find out one simple action you can perform on a regular basis that will substantially reduce the probability of users compromising the network and will provide you with the metrics to show this reduction to your senior management. **Speaker: Stuart Wagner, Director, IT Security & Compliance, Enterprise Products** **K6 B: Phishing your employees: Lessons learned from phishing over 3.5 million people** Cyber crime and electronic espionage, most commonly, initiate with an employee clicking a link to a website hosting malware, opening a file attached to an email and laden with malware, or just simply giving up corporate credentials when solicited via phishing websites. Phishing has been used to hijack online brokerage accounts to aid pump n' dump stock scams, compromise government networks, sabotage defense contracts, steal proprietary information on oil contracts worth billions, and break into the world's largest technology companies to compromise their intellectual property. Technical controls presented as silver bullets provide false hope and a false sense of security to employees, promoting dangerous behaviors. Learn how to build a scalable and effective program to educate your staff and change behavior from experts at PhishMe. **Speaker: Jim Hansen, VP, PhishMe** **Moderators: Mario Chiock, Schlumberger & Jessica Garrison, Shell**	
5:00 PM	**Adjourn**	
5:00 – 6:00 PM	**Reception and Networking – *Sponsored by Venafi***	