SINET ITSEF
IT Security Entrepreneurs Forum

The Computer History Museum, Silicon Valley
April 19 & 20, 2016

Supported by the US Department of Homeland Security Science & Technology Directorate
Thank You to Our Generous Sponsors

FOUNDING SPONSORS

Homeland Security
Science and Technology

KAUFFMAN
The Foundation of Entrepreneurship
GOLD SPONSORS

Bay Dynamics

General Dynamics
Mission Systems

Gigamon

SIDLEY
150 YEARS

Complete list of sponsors on page 22–25
Dear SINET Community,

As we celebrate our tenth annual ITSEF I wanted to thank you for being a part of our community of interest and trust. SINET’s success isn’t about us, but rather all of you who make up the fabric of our global network — the builders, buyers, policymakers, investors and researchers.

I’m excited about our program that brings to light industry and government’s most pressing needs and priorities. You’ll be taken along the journey of the entrepreneur, listen and participate in the debate on privacy verse security, learn the promise and peril of our connected world, and discuss current topics of interest in One-on-One meetings and the Information Sharing Hour hosted by thought leaders from industry, government and the investment communities. It’s certainly going to be a memorable event.

The continuing barrage of sophisticated attacks are driving the need for increased capital investment, further dedicated R&D funding, more security focused acquisitions, an influx of government and system integrators establishing new offices in Silicon Valley and other centers of innovation. In addition, stronger Cybersecurity policy legislation, both domestically and globally are indicators that this market is not going away anytime soon.

As SINET continues to connect the ecosystem of the entrepreneur in Silicon Valley, Washington DC, New York City, London and now Sydney, it is imperative that we strive to bring more innovative solutions to market, embrace early adoption, continue to share information and not forget to share our most cutting edge solutions with our trusted industry and government allies in order to protect ourselves from the adversary.

I would like to extend a special thank you to the Department of Homeland Security S&T Directorate, in particular Dr. Douglas Maughan, our sponsors and distinguished speakers, SINET members, and to all of our valued SINET community. I’m grateful that you are joining us as we continue to build communities of interest and trust that support the advancement of Cybersecurity innovation. We appreciate you being a part of our SINET family and could not do this without you…

Sincerely,

Robert D. Rodriguez
SINET Chairman & Founder
ITSEF Agenda

April 19, 2016
Day One

12:00 PM – 1:00 PM
Registration

1:00 PM – 2:00 PM
General Session
HAHN AUDITORIUM

1:00 PM – 1:05 PM
Introductory Remarks
• Rick Geritz, Chief Executive Officer & Founder, Life Journey, Chairman, CyberMaryland

1:05 PM – 1:15 PM
Welcome Remarks
• Robert D. Rodriguez, Chairman & Founder, SINET
How to Use the Military Observe, Orient, Decide, and Act Approach to Operationalize Cyber Risk Management

Abstract: To respond to mounting cyber-attacks, advanced persistent threats, and insider leaks, enterprises and government entities need reliable, real-time visibility into their IT security posture. However, most traditional security tools are silo-based and require legions of staff to comb through the huge amount of data to connect the dots and find the needle in the haystack. These efforts can take months, during which time attackers can exploit vulnerabilities and extract data. Breaking down silos and automating security operations tasks is therefore essential for implementing a new enterprise security model. To address these challenges, progressive organizations are exploring how the military concept of the OODA (Observe, Orient, Decide, Act) Loop can be applied in day-to-day cyber risk management operations to identify, visualize, prioritize, and orchestrate the remediation of cyber risks across the entire computing stack in near real time. Dr. Mukkamala will illustrate how to operationalize a new, pro-active model to cyber risk management based on the four step OODA Loop concept:

**Observe**
Through automated aggregation of data across different data types; mapping of assessment data to compliance requirements; and normalization for ruling out false-positives, duplicates, and to enrich data attributes.

**Orient**
By placing internal security intelligence, external threat data, and business criticality into context to derive a holistic view of risk posture across the entire IT stack.

**Decide**
By applying advanced risk scoring and machine-learning technology to assign different levels of risk to assets, applications, and business processes as well as enabling interactive drill-down and visualizations of correlated data and visualization of application attack path analysis.

**Act**
Using built-in workflow, ticketing, and remediation capabilities, with detailed remediation steps for each vulnerability, to automate real-time risk management.

Moderator:
- **Dr. Srinivas Mukkamala**, CEO, RiskSense

Panelists:
- **Mark Bregman**, CTO, NetApp
- **Capt. Brandon Johns**, USCYBERCOM, Silicon Valley Points of Partnership Team
- **Dave Mahon**, VP & Chief Security Officer, CenturyLink
Track Sessions

**TRACK A:** 2:00 PM – 2:45 PM
HAHN AUDITORIUM

Adversarial Modeling to Develop Effective Defenses

**Abstract:** The question CISOs get from their CEOs and Boards often after headline making breaches is “How secure are we?” Being able to answer the question quantitatively has been elusive in cyber security because the field has grown up in a relatively ad hoc fashion rather than as an engineered discipline. Marketing by vendors tends to dominate rigor in creating architectures and solutions to threats an enterprise faces.

In this panel, we discuss recent initiatives in developing adversarial models and their associated playbooks, and then running these against defense-in-depth architectures to evaluate coverage gaps. The answer to “how secure are we” is only answerable with respect to an adversarial model and the attacks that may be employed against you. A panel of distinguished CISOs, industry experts, and threat intelligence analysts will discuss the role in adversarial modeling to improve enterprise defenses.

**Moderator:**
- **Anup Ghosh**, Founder & Chief Executive Officer, Invincea

**Panelists:**
- **Paul Calatayud**, Chief Information Security Officer, SureScripts
- **Taher Elgamal**, Chief Technology Officer, Salesforce
- **Rick Howard**, Chief Information Security Officer, Palo Alto Networks
- **Philip Reitinger**, President and Chief Executive Officer, Global Cyber Alliance

**TRACK B:** 2:00 PM – 2:45 PM
GRAND HALL

The Last ‘Unicorns’ – The Art and Science of Alternative Exits

**Abstract:** In Silicon Valley, the exit is celebrated. The tech industry refers to rising star companies as “unicorns” because they are special and valuable. Yet one must not forget that they are valuable precisely because they are rare. No one likes a sad ending, but the vast majority of ventures do not make it to anywhere near unicorn valuations. And failure is generally only celebrated when followed by a dramatic success. So when is it right to exit? What are the alternatives to the conventional VC trajectory? This panel will discuss the art and science of the exit with a focus on alternatives to traditional VC unicorn mythology. What of a private equity approach vs. VC? Early acquisition by a strategic buyer vs. building to beat the establishment? Are we seeing a trend toward early stage acquisitions? Is selling early selling out? Our panel includes experts who understand the rarity of ‘unicorns’ and the value of alternative exits. Leading investment bankers, recently exited founders and PE investors will share insight into the art and science of exits.

**Moderator:**
- **Peter LaMontagne**, Chief Executive Officer, Novetta Solutions

**Panelists:**
- **Eric Benhamou**, Founder & General Partner, Benhamou Global Ventures
- **Maria Lewis Kussmaul**, Co-Founder & Partner, AGC Partners
- **Enrique Salem**, Managing Director, Bain Capital Ventures
- **Cack Wilhelm**, Principal, Scale Venture Partners

2:45 PM – 3:10 PM

Break
**TRACK A:** 3:10 PM – 3:55 PM  
HAHN AUDITORIUM

Quantifying Cyber Risk: A Manual for Holistic Enterprise Risk and Senior Security Professionals

**Abstract:** Cyber risk is just that, an element of risk facing the entire enterprise — not limited to IT. As such, Cybersecurity needs to be thought of with an intelligence and business process mindset. The moderator’s Cybersecurity analysis work with F1000 organizations has helped foster best practices towards evaluating and measuring Cybersecurity risk as a whole. Chris will lead a discussion with expert panelists in sharing their best practices with the audience, stressing the value of evaluating Cybersecurity as part of risk response, and in context of network resources, assets and the regulatory environment. Audience members will learn:

- How to understand what’s on their network – depth and breadth of assets and applications
- The importance of the two S’s: scalability and speed
- The value and roles of both internal and external threat intelligence data
- How to enable efficient and effective decision making and integrate cyber issues into holistic discussions on risk, including regulatory requirements.

**Moderator:**
- Chris Morgan, Co-Founder and Chief Technology Officer, IKANOW

**Panelists:**
- Renee Guttmann-Stark, Chief Information Security Officer, Royal Caribbean Cruise
- Brian Johnson, Chief Information Security Officer, Lending Club
- Nathan Lesser, Deputy Director, National Cybersecurity Center of Excellence National Institute of Standards and Technology
- Valmiki Mukherjee, Chairman & Founder, Cyber Future Foundation & Constituents

**TRACK B:** 3:10 PM – 3:55 PM  
GRAND HALL

IoT Cybersecurity – How Do We Protect the World with Limited Resources

**Abstract:** The emergence of the Internet of Things (IoT), with billions of unmonitored devices have embedded network connectivity and is bringing a quantum leap into the complexity of our IT systems and increasing the challenge of defending them. Compounding this problem are threats embedded in hardware and firmware. Currently undetectable by traditional security tools, these threats are expected to become more prevalent in this era of machine-to-machine networking. The result is a growing window of opportunity for hackers, criminals and nation states to exploit breaches in critical information systems. Tales have emerged of backdoors inserted by Chinese manufacturers into chips for use by the U.S. military and medical device hacking has been silently going on for some time. The ability to interfere with medical devices or onboard vehicle systems in increasingly sophisticated smart cars obviously could be disastrous. As a result, there often is little physical space, little virtual space for memory, limited power and limited bandwidth. These constraints put a premium on efficiency for any IoT security solution. This panel will investigate real risks associated with ubiquitous IoT and the need for new approaches to IoT cybersecurity.

**Moderator:**
- Steven Chen, Chief Executive Officer, PFP Cybersecurity

**Panelists:**
- Grant Babb, Research Scientist - Security Data Scientist, Intel Corporation
- Vijay Dheap, Program Director, IBM Master Inventor, QRadar Emerging Initiatives - Cyber Forensics, SaaS, Managed Services, IBM
- Benjamin Goldsmith, Cyber Security Advisor, Office of the Deputy Under Secretary for Cybersecurity & Communications
- Dan Isaacs, Director of Connected Control, Xilinx
- Randy Miskanic, Chief Information Security Officer and Vice President Digital Solutions, U.S. Postal Service
**TRACK A: 3:55 PM – 4:40 PM**
**HAHN AUDITORIUM**

**Securing the Enterprise from New Attack Vectors Using Software-Defined-Radios with Big Data Analytics**

**Abstract:** We are now in the age of digital business, where the Internet of Things (IoT) and cloud computing provides expanded options for organizations to deliver value. But digital business depends on a digital infrastructure, and a digital infrastructure must be secure to avoid risk. IoT must not only save money and provide more options—it must do so securely and safely to be truly effective. The Internet of Things (IoT), a mish-mash of converging operating systems, wireless protocols and embedded processors has turned heating, ventilation and air conditioning systems, photocopiers, printers and scanners into “smart devices,” able to transmit data to smart phones and amongst themselves. Threats are evolving, becoming increasingly sophisticated and more numerous. Traditional approaches to securing IT systems have expanded to include new requirements to meet the additional demands of operational technology and the Internet of Things. This panel will discuss the problems associated with wireless and mobile technologies: as more devices become Internet-enabled, they can be used as a gateway to hack into a company’s IT network to steal data, or bring down the network connected system. The IoT device can become an infection vector so we will review some best practices for future proofing your cybersecurity check-lists.

**Moderator:**
- **Garry Drummond**, Founder & Chief Executive Officer, 802 Secure, Inc.

**Panelists:**
- **Tina Hampton**, Vice President Cybersecurity Innovation & Strategy, AT&T
- **Mike Raggo**, Director of Security Research and MobileIron Security Labs, MobileIron
- **Richard Rushing**, Chief Security Officer, Motorola

---

**TRACK B: 3:55 PM – 4:40 PM**
**GRAND HALL**

**The Journey of the Entrepreneur: Trials and Tribulations**

**Abstract:** If you asked 10 entrepreneurs what the biggest hurdle to starting a company was, chances are you’d get 10 different answers. The reason is simple. Every entrepreneur faces different obstacles or has different challenges to overcome when building a new business. But while there will always be challenges that are unique to each individual, there are also common obstacles that every entrepreneur will face at one point or another. Whether it’s when to seek investment, where to locate your headquarters, how to attract new talent, determining when (or if) to bring in additional management, etc. Every entrepreneur will face these decisions at some point, but being prepared can make all the difference in whether that challenge becomes a stumbling block or a stepping stone. In this session you’ll hear from real entrepreneurs who faced each of these challenges and get their unique insights on how to confront them, when to confront them, and the best strategies for keeping your business on track.

**Moderator:**
- **Hank Barry**, Co-Chair, Emerging Companies and Venture Capital Practice Group, Sidley Austin LLP

**Panelists:**
- **C. Bryce Benjamin**, Principal, Alta Ventures
- **Marcin Kieczynski**, Chief Executive Officer, Malwarebytes
- **Hugh, Njemanze**, Founder and Chief Executive Officer, Anomali
- **Tomer Weingarten**, CEO & Co-Founder, SentinelOne
**TRACK A:** 4:40 PM – 5:25 PM  
HAHN AUDITORIUM

How to Filter Noise and See Signals in the Security Industry

Abstract: All products and services are not created equal, but today’s security industry is filled with messages that increasingly sound the same. Adopting the wrong strategies and solutions can sink reputations, organizations, investments, and careers. Fresh solutions are essential to staying ahead of the threats, but finding them takes patience, critical resources, and industry awareness—even for the largest enterprises. Small and medium enterprises face an even greater challenge with limited budgets, experience, and access to talent.

- How are large enterprise CISOs battling this noise?
- What is their process for finding and trialing new solutions?
- What are the technology and organizational challenges in overcoming the deluge of “event” data?
- How are entrepreneurs on the cutting edge able to gain the attention of the market?
- What resources are available to small and medium enterprises to find solutions that fit their needs and constraints?

The panelists will discuss their strategies for identifying new solutions and filtering through the noise.

Moderator:
- **Sam Small**, Chief Executive Officer  
  Fast Orientation, Inc.

Panelists:
- **Brad Arkin**, CISO, Adobe
- **Shardul Shah**, Partner, Index Ventures
- **Joe Voje**, CISO, City of San Francisco
- **Mike Wilson**, CISO, McKesson

**TRACK B:** 4:40 PM – 5:25 PM  
GRAND HALL

Federal Cybersecurity Spending: What is the Real Market for the Private Sector?

Abstract: The Federal market is NOT like the commercial market. It requires a different sales strategy and approach. One must understand the Federal market in order to be successful in it. How much money is the Federal government spending on cyber security? How much is unclassified spending on cyber security? How much is addressable to the private sector? If I’m new to the Federal market, how do I get into that market? This session will provide an overview of cyber security mission and cyber security spending, priority areas, major buyers/spenders, and what is addressable to the private sector. Pragmatic guidance and suggestions will be offered regarding doing business with the Federal government.

- **Justin Taft**, President and Chief Executive Officer, The Soter Group

5:25 PM

Adjournment
Day Two
April 20, 2016

7:30 AM – 8:30 AM
Registration and Continental Breakfast

8:30 AM – 5:30 PM
General Session
HAHN AUDITORIUM

8:30 AM – 8:35 AM
Introductory Remarks by Forum Host
• Rick Geritz, President & Founder, LifeJourney and Chairman, CyberMaryland

8:35 AM – 8:50 AM
Welcome Remarks
• Dr. Douglas Maughan, Director, Cyber Security Division, DHS Science & Technology Directorate

8:50 AM – 9:15 AM
Keynote
• The Honourable Harjit Singh Sajjan MP, Minister of National Defence, Canada
9:15 AM – 10:00 AM

Cloud, Containerization and Micro-Services—What Do Security Professionals Need to do to Keep their Organizations Safe

Abstract: Cloud is no longer a passing fad. The first generation of cloud adoption was mostly driven by the need to drive cost out of organizations. General consensus is we are now in the second generation of cloud. This phase will be driven by the need for large organizations to take advantage of the new capabilities and advanced technologies available in the cloud. Even regulators are becoming more accepting of the cloud. As more organizations look to the cloud, at the end of the day you cannot outsource accountability, so what do CISO’s need to do in-order to keep their organizations safe? As part of this panel we will discuss:

- The importance of contractual agreements
- How to evolve your architecture for the cloud
- Regulated Industries in the cloud
- Key security considerations
- Disaster Recovery
- Dev Ops
- Incident Response

Moderator:
- David Cass, Chief Information Security Officer Cloud & SaaS Operational Services, IBM

Panelists:
- Niall Browne, Chief Trust Officer & VP Trust, Workday
- Brian Done, Chief Architect / Senior Strategist, Office of Cyber Security and Communications, DHS
- Janice Haith, Director, Deputy Department of Navy Chief Information Officer, U.S. Navy
- Erik Naugle, Director of Cloud and Internal Hosting Security, Intuit

10:00 AM – 10:15 AM

SINET Thinks Forward with Scott Wilkie: Converting Cyber Innovation into High Value Enterprise Solutions

Abstract: In a rapidly changing world, both public sector and enterprise frequently state that cyber innovators only address their needs at the edge leading to low rates of adoption of new technologies and processes. This session will address the opportunity for a greater understanding of future industry dynamics and user needs, individually and collectively, to develop and protect business value. As Australia’s National Data Agency, Data 61 has recently published key reports about the “Future of Work” and “Global Megatrends: Seven Patterns of Change Shaping Our Future” aligned with the National Innovation and Cyber Agendas to create an environment for better use outcomes.

- How do innovators learn more about what buyers really want?
- Is innovation really possible in a hyper-secure world?
- Is innovation valuable without cultural change?
- How can we quantify risk vs. return when it comes to cyber and what new solutions or industries will arise?

Moderator:
- Scott Wilkie, Senior Advisor, Data61

10:15 AM – 10:35 AM

Break
Balancing Privacy and Security in a Connected Digital World

Abstract: Ben Franklin famously stated in 1755: “Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety.”

Some 261 years later, the debate over balancing privacy with security remains a lively and critical discussion. Can we protect the public’s safety while at the same time respecting their privacy? Is America really safer with end-to-end encryption? Should privacy laws and policies lean towards the needs of US Law Enforcement and other security agencies in order to keep us safer? At the center of this debate is the Apple verse FBI battle. A recent poll conducted by the Pew Research Center found that 51% felt that Apple should unlock the iPhone, while only 38% said they should not. Where do you stand? Please join these panelists for a stimulating discussion on balancing privacy and security and why it is important.

Moderator:
• Ari Schwartz, Managing Director of Cybersecurity Services, Venable, LLC

Panelists:
• Dan Boneh, Professor of Computer Science & Electrical Engineering, Stanford University
• Aaron Mackey, Frank Stanton Legal Fellow, Electronic Frontier Foundation
• Cornelius Tate, Vice President, Asset Protection & Incident Response, Sallie Mae Bank
• Stuart Tryon, Special Agent in Charge, U.S. Secret Service

SINET Thinks Forward with Micha Benoliel: FireChat—The Power of Social Mesh

Abstract: Join Micha as he tells the story of FireChat, the first messaging app that works when there is no internet access and discusses the power of social mesh and how it has been used during political events, internet shut down and disaster recovery situations.

• Micha Benoliel, FireChat Creator, Founder @OpenGarden

Military & Civilian Government Challenges in Cybersecurity

Abstract: Moving beyond “conventional IT” such as local area networks (LANs) and wide area networks (WANs), we encounter different issues associated with securing and protecting real-time control systems. For instance, in the case of a weapons/control system, the traditional security attributes (confidentiality, integrity, availability) often need to be inverted in importance (availability, integrity, confidentiality). Availability becomes preeminent, because a “real-time” control system usually cannot be disturbed while in operation. This has implications for activities such as scanning, patching, and continuous monitoring where latency is an issue. How should we do these important activities for our tactical IT control systems? Are technological solutions or techniques already available? Further, tactical systems are more difficult to upgrade or even change due to their deterministic functions. When you press “button A” you expect “action B.” No exceptions. Therefore, any changes to the system must be verified and tested to ensure predictable operation, in each of the numerous configurations where the systems operate. Changes must occur in a controlled environment and with the right expertise present to address problems as opposed to implementing at sea in the operating forces. This is just one example of several to be discussed.

Moderator:
• Louis Parks, President & CEO, SecureRF Corporation

Panelists:
• Vice Admiral Ted N. Branch, Chief Information Officer, Director of Cybersecurity, U.S. Navy LT General
• Robert Ferrell, CIO, U.S. Army
• Peter Gouldmann, Director of IT Security Compliance, U.S. Department of State
Networking Luncheon Table Hosts

A complete list of lunch table topics can be found on pages 18 & 19.

HANK BARRY—TABLE #1
Co-Chair, Emerging Companies and Venture Capital Practice Group
Sidley Austin

JAMES BEESON—TABLE #2
Chief Information Security Officer
GE Capital Americas

DAN BONEH—TABLE #3
Professor of Computer Science
Stanford University

VICE ADMIRAL TED N. BRANCH—TABLE #4
US Navy’s Chief Information Officer
Director of Navy Cybersecurity
US Navy

NIAIL BROWNE—TABLE #5
Chief Trust Officer
Workday

DAN DAGHER—TABLE #6
DoD CIO Cybersecurity Strategy
Pentagon (C)

JANICE HAITH—TABLE #6
Director
Department of Navy Deputy Chief Information Officer

MARY ANN DAVIDSON—TABLE #7
Chief Security Officer
Oracle Corporation

TIM DOMBROWKSI—TABLE #8
Chief Executive Officer
Airbus Ventures

TAHAR ELGAMAL—TABLE #9
Chief Security Officer
Salesforce

LEE GRAUL—TABLE #10
Project Manager
National Security Agency
Ft. Meade, Maryland
KIM GREEN—TABLE #11
Chief Information Security & Privacy Officer
Zephyr Health

RENEE GUTTMANN-STARK—TABLE #12
Chief Information Security Officer
Royal Caribbean Cruise

PATRICK HEIM—TABLE #13
Head of Trust & Security
Dropbox

AARON JACOBSON—TABLE #14
Venture Investor
NEA

MARIA LEWIS KUSSMAUL—
TABLE #15
Co-Founder & Partner
AGC Partners

DR. ZULFIKAR RAMZAN—TABLE #16
Chief Technology Officer
RSA, The Security Division of EMC

RICHARD RUSHING—TABLE #17
Chief Security Officer
Motorola

REYNOLD SCHWEICKHARDT—TABLE #18
Director of Technology Policy
Committee on House Administration

SONNY SINHA—TABLE #19
Committee on House Administration

DAVE ZILBERMAN—TABLE #20
Partner
Comcast Ventures

ROBERT PATE—TABLE #21
Executive Vice President for Strategic Development & Cybersecurity
Cloudburst Security

NICK SHEVELYOV—TABLE #21
Chief Security Officer
Silicon Valley Bank
Maximize this 75-minute luncheon by sitting down in an informal and intimate setting with distinguished security thought leaders and experts. Topics will focus on how solution providers can best shape their business strategies to meet the needs of the market.

- **Table #1: Hank Barry**, Co-Chair, Emerging Companies & Venture Capital Practice Group, Sidley Austin  
  **Topic:** Open Mic – Discussing Today’s News

- **Table #2: James Beeson**, Chief Information Security Officer, GE Capital Americas  
  **Topic:** Attracting and Keeping Security Talent

- **Table #3: Dan Boneh**, Professor of Computer Science and Electrical Engineering, Stanford University  
  **Topic:** Recent Developments in Computer Security

- **Table #4: Vice Admiral Ted Branch**, Chief Information Officer, Director of Cybersecurity, U.S. Navy  
  **Topic:** Navy Cyber Resiliency in Warfighting

- **Table #5: Niall Browne**, Chief Trust Officer, Workday  
  **Topic:** The Security Benefits of Moving to The Cloud

- **Table #6: Dan Dagher**, DoD CIO Cybersecurity Strategy, Pentagon  
  **Table #6: Janice Haith**, Director, Deputy Department of Navy Chief Information Officer, U.S. Navy  
  **Topic:** Industry Certification and Accreditation: Rapid Reciprocity

- **Table #7: Mary Ann Davidson**, Chief Security Officer, Oracle Corporation  
  **Topic:** Building Better Code

- **Table #8: Tim Dombrowski**, Airbus Ventures  
  **Topic:** Security from Commercial Drone Attacks

- **Table #9: Tahar Elgamal**, Chief Security Officer, Salesforce  
  **Topic:** Is the Cloud More Secure?

- **Table #10: Lee Graul**, Program Manager, NSA/CSS Commercial Solutions Center (NCSC, National Security Agency)  
  **Topic:** A Conversation about Cybersecurity Information Sharing

- **Table #11: Kim Green**, Chief Information Security & Privacy Officer, Zephyr Health  
  **Topic:** Does It Stay or Go? And, Why Would We Risk Doing Business with a Start Up?

- **Table #12: Renee Guttmann-Stark**, Chief Information Security Officer, Royal Caribbean Cruise  
  **Topic:** Build vs. Buy? Making Decisions on Security Investments

- **Table #13: Patrick Heim**, Head of Trust & Security, Dropbox  
  **Topic:** Venture Investing in Cybersecurity: Key Themes for 2016

- **Table #14: Aaron Jacobson**, Venture Investor, NEA  
  **Topic:** The M&A Environment in the Cyber Sector

- **Table #15: Maria Lewis Kussmaul**, Co-Founder & Partner, AGC Partners  
  **Topic:** How Should We Think About Security in a Post-Prevention World?
• **Table #17: Richard Rushing**, Chief Security Officer, Motorola  
  **Topic**: Can You Win Against Cyber Crime?

• **Table #18: Reynold Schweickhardt**, Director of Technology Policy, Committee on House Administration  
  **Topic**: How to Address Targeting of Key Staff in Their Personal Lives

• **Table #19: Sonny Sinha**, President, Sinha Associates LLC  
  **Topic**: The President’s Cybersecurity National Action Plan

• **Table #20: David Zilberman**, Partner, Comcast Ventures  
  **Topic**: Funding Environment for Cybersecurity Start-ups

• **Table #21: Nick Shevelyov**, Chief Security Officer, Silicon Valley Bank  
  **Robert Pate**, Executive Vice President for Strategic Development & Cybersecurity, Cloudburst Security  
  **Topic**: Cybersecurity Shark Tank  
  **Abstract**: Innovators at this table will be given the opportunity to deliver their best two-minute elevator pitch on their Cybersecurity product or service they are providing into the marketplace. Nick and Robert will provide feedback and counsel to these entrepreneurs on ways they may be able to advance their offerings, adjustments to their current roadmap as well as the opportunity to be invited into future customer meetings if they are a winner during their time in the Shark Tank.

### 1:40 PM – 5:30 PM

**General Session**  
**HAHN AUDITORIUM**

### 1:40 PM – 1:55 PM

**SINET Thinks Forward with Nick Shevelyov: “Blind Spots” – An Interactive Discussion on Issues Creating Security Risks for Organizations Outside of the Typical Cyber Security Challenges**  
**Abstract**: Normalization of risk deviation, technical debt, thinking fast when you should be Thinking Slow…the road to hell is paved with good intentions and this discussion will address some of these blind spots creating systemic risk in enterprises.

• **Nick Shevelyov**, Chief Security Officer, Silicon Valley Bank

### 1:55 PM – 2:15 PM

**SINET Thinks Forward with Dan Roam: The Back of the Napkin: Using Simple Pictures to Explain Complex Security Concepts**  
**Abstract**: In this fast-paced and highly visual session, international best-selling author Dan Roam will show how simple pictures are the mind’s most powerful way to explain complex concepts quickly — including information security challenges. In minutes, Dan will show how a basic understanding of the neuromechanics of vision can help you break down the most complex of your ideas into a series of simple pictures which are easy to create and powerful to share.

• **Dan Roam**, President, Digital Roam Inc.
2:15 PM – 3:00 PM

The Evolution of Risk Management in the Enterprise: From the C-Suite to Technology to Operations

**Abstract:** Security management in corporate enterprises is changing. As the types and uses of technology evolve and threats & vulnerabilities persist, companies must shift how they identify, categorize and respond to cybersecurity risks. This shift requires a strategic, business-centric approach that integrates risk assessments and mitigations into ongoing business practices and does not rely solely on the IT department for security.

This expert panel of Chief Information Security Officers will discuss how their respective organizations are using risk-based approaches to managing IT security. Today's successful programs require direct collaboration with non-IT leaders, communication with the Board of Directors and establishing mechanisms to assess risks and prioritize an organization’s protections. The audience will learn how a diverse set of organizations are managing IT security, the challenges associated with developing a risk-centric approach, and the potential that such approaches provides.

**Moderator:**
- Joel Molinoff, Senior Vice President, Chief Information Security Officer, CBS Corporation

**Panelists:**
- Reggie Davis, General Counsel, DocuSign
- Michael Golz, Chief Information Officer, Americas, SAP
- Phil Quade, Special Assistant to Director NSA for Cyber, Chief of NSA, National Security Agency

3:00 PM – 3:15 PM

SINET Thinks Forward with Joe Sullivan: Good Security Requires Innovation

**Abstract:** Joe Sullivan has learned through career stops at the US DOJ, eBay, Facebook, and now Uber that you cannot build a great security program without creating a strong culture of innovation within that team, with a willingness to try new ideas, and a comfort with being transparent about your successes and failures. In this time of unprecedented business innovation, we as security professionals must more than match the speed of development across our businesses and communities to provide sufficient security to help our businesses succeed.

- Joe Sullivan, Chief Security Officer, Uber

3:15 PM – 3:35 PM

Break

3:35 PM – 4:20 PM

Identifying Hacked Networks and Response Strategies

**Abstract:** Traditional enterprise security strategies are largely focused on defensive tactics and authentication layers. While a solid defensive strategy remains necessary, we would like to explore and discuss strategies relative to how companies positively identify if they have been compromised. And, if so, what their tactical strategies are for managing or responding to the threat.

**Moderator:**
- Rick Orloff, Chief Security Officer, Code 42

**Panelists:**
- Neil Boland, VP Information Security, Major League Baseball
- Logan Browne, Chief Technologist, Hewlett-Packard
- Patty Hatter, Vice President & General Manager of Professional Services, Intel
- Dan Schott, Head of Global Fraud Investigations, VISA
4:20 PM – 4:40 PM

**SINET Thinks Forward with Gerhard Eschelbeck: My Role at Google**

**Abstract:** What's it like heading up security for one of the world's biggest tech companies and hacker targets? Google VP of Security Engineering Gerhard Eschelbeck will give a rare inside look at his daily job, how he protects the data of millions of people and companies, the big and little challenges Google faces with security and what keeps him up at night.

- Gerhard Eschelbeck, Vice President Security & Privacy Engineering, Google

4:40 PM – 5:25 PM

**The When, What and Why of How CISOs Buy**

**Abstract:** Not everyone gets a first meeting and even less get a second meeting. These CISOs will share their model for what a successful meeting looks like and how you can improve your chances for that critical second meeting that leads to the next step, the Pilot.

**Moderator:**
- Matt Howard, Managing Partner, Norwest Venture Partners

**Panelists:**
- James Beeson, CISO and IT Risk Officer, GE Capital Americas
- Kim Green, Chief Information Security and Privacy Officer, Zephyr Health
- Patrick Heim, Head of Trust & Security, Dropbox

5:25 PM – 5:30 PM

**Closing Remarks**

- Robert D. Rodriguez, Chairman & Founder, SINET

5:30 PM – 7:30 PM

**SINET Connects: Networking Reception**
Thank you to the SINET ITSEF & Workshops 2016 Sponsors

FOUNDING SPONSORS

Homeland Security
Science and Technology

KAUFFMAN
The Foundation of Entrepreneurship
GOLD SPONSORS

Bay Dynamics

DATA 61

CSIRO

GENERAL DYNAMICS
Mission Systems

Gigamon

SIDLEY 150 YEARS
SILVER SPONSORS

ANOMALI

AGC PARTNERS

cyberpoint

invincea™

Google

MACH37™ CYBER ACCELERATOR

Malwarebytes

NOVETTA

paloalto NETWORKS®

the network security company™

RISKIQ™
EMERGING SPONSORS

- CyberSpone
- Fast Orientation
- LiFARS
- RedOwl Analytics
- Reversing Labs
- RiskSense, Inc.
- SAINT
- ThreatConnect

MEDIA SPONSOR

The CyberWire
DO YOU HAVE CUTTING EDGE TECHNOLOGY?

Innovative solutions frequently come from new and small companies. Our goal is to provide entrepreneurs from all over the world an opportunity to increase their product awareness to a select audience of sophisticated investors, builders and buyers. In order to participate, companies must have annual revenues of approximately fifteen (15) Million dollars or less.

BENEFITS OF APPLYING TO BE SELECTED AS ONE OF THIS YEAR’S SINET 16 INNOVATORS:

• SINET 16 Innovators will have six minutes to deliver their value proposition on stage in front of 300 to 400 investors, builders, buyers and researchers;
• SINET 16 Innovators will be included in SINET press releases and marketing material before, during and after the Showcase;
• SINET 16 Innovators will receive a free booth to display their technology at the Showcase on November 4th;
• SINET 16 Innovators will receive free but mandatory coaching on their messaging for the November 4th stage presentation;
• SINET 16 Innovators will enjoy additional opportunities to present at other SINET supported global venues that may arise throughout the year (TBD).

THE SINET 16 PROCESS FOR 2016:

In preparation for the SINET Showcase, SINET assembles a steering committee consisting of Cybersecurity leaders from industry, government, venture capital, investment banking and academia. Our esteemed committee works with Federal Agencies and private industry to identify their most critical needs and requirements. These needs and requirements are used to help evaluate the company’s application during the vetting process.

• June 20, 2016: SINET 16 Innovator application process will close. No applications will be accepted after this date.
• September 15, 2016: the final list of this year’s SINET 16 Innovators will be notified that they have been selected to present on stage at the 2016 SINET Showcase in Washington, DC.
• October 10-12, 2016: The companies selected will receive free coaching on their presentation skills on the East Coast in Rosslyn, Virginia and on the West Coast in Menlo Park, California. (This coaching is complimentary but mandatory in order to maximize the presenters six minutes on stage).
• November 2, 2016: SINET 16 Innovators will have an opportunity to meet with interested parties at their booth throughout the day and during the two- hour evening reception.

For additional SINET 16 application process questions, please contact Bill Bosen | billbosen@security-innovation.org
Speakers
SINET Speakers

Complete speaker bios can be found at http://www.security-innovation.org/ITSEF_2016-Speakers.htm

KEYNOTE SPEAKER

THE HONOURABLE HARJIT SINGH SAJJAN MP
Minster of National Defence
Canada

SINET CHAIRMAN AND FOUNDER

ROBERT D. RODRIGUEZ
Chairman and Founder
SINET

SPEAKERS

BRAD ARKIN
CISO
Adobe

GRANT BABB
Research Scientist
Security Data Scientist
Intel Corporation

HANK BARRY
Co-Chair, Emerging Companies and Venture Capital Practice Group
Sidley Austin

JAMES BEESON
Chief Information Security Officer
GE Capital Americas

ERIC BENHAMOU
Founder & General Partner
Benhamou Global Ventures

C. BRYCE BENJAMIN
Principal
Alta Ventures
<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Company/Institution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mica Benoliel</td>
<td>Chief Executive Officer</td>
<td>Open Garden</td>
</tr>
<tr>
<td>Neil Boland</td>
<td>VP Information Security</td>
<td>Major League Baseball</td>
</tr>
<tr>
<td>Dan Boneh</td>
<td>Professor of Computer Science</td>
<td>Stanford University</td>
</tr>
<tr>
<td>Vice Admiral Ted N. Branch</td>
<td>US Navy’s Chief Information Officer</td>
<td>US Navy</td>
</tr>
<tr>
<td>Mark Bregman</td>
<td>CTO</td>
<td>NetApp</td>
</tr>
<tr>
<td>Logan Browne</td>
<td>Chief Technologist and Director</td>
<td>HPE Cyber Security Architecture and Engineering</td>
</tr>
<tr>
<td>Niall Browne</td>
<td>Chief Trust Officer</td>
<td>Workday</td>
</tr>
<tr>
<td>Paul Calatayud</td>
<td>Head of Information Security, Audit, Compliance and Enterprise Risk Management, Chief Information Security Officer</td>
<td>Surescripts</td>
</tr>
<tr>
<td>David A. Cass</td>
<td>Chief Information Security Officer</td>
<td>IBM</td>
</tr>
<tr>
<td>Steven Chen</td>
<td>Chief Executive Officer</td>
<td>PVP Cybersecurity</td>
</tr>
<tr>
<td>Reggie Davis</td>
<td>General Counsel</td>
<td>DocuSign</td>
</tr>
<tr>
<td>Vijay Dheap</td>
<td>Program Director, IBM Master Inventor</td>
<td>QRadar Emerging Initiatives—Cyber Forensics, SaaS, Managed Services</td>
</tr>
<tr>
<td>Brian Done</td>
<td>Chief Architect / Senior Strategian</td>
<td>Office of Cyber Security and Communications</td>
</tr>
</tbody>
</table>

SINET ITSEF 2016
<table>
<thead>
<tr>
<th>Name</th>
<th>Title/Company</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patrick Heim</td>
<td>Head of Trust &amp; Security, Dropbox</td>
</tr>
<tr>
<td>Matt Howard</td>
<td>Managing Partner, Norwest Ventures</td>
</tr>
<tr>
<td>Rick Howard</td>
<td>Chief Security Officer, Palo Alto Networks</td>
</tr>
<tr>
<td>Dan Isaacs</td>
<td>Director of Connected Control, Xilinx</td>
</tr>
<tr>
<td>Capt. Brandon Johns</td>
<td>USCYBERCOM, Silicon Valley Points of Partnership Team</td>
</tr>
<tr>
<td>Brian Johnson</td>
<td>Chief Information Security Officer, Lending Club</td>
</tr>
<tr>
<td>Marcin Kleczyński</td>
<td>Chief Executive Officer and Founder, Malwarebytes</td>
</tr>
<tr>
<td>Peter Lamontagne</td>
<td>Chief Executive Officer, Novetta Solutions</td>
</tr>
<tr>
<td>Nathan Lesser</td>
<td>Deputy Director, National Cybersecurity Center of Excellence National Institute of Standards and Technology</td>
</tr>
<tr>
<td>Maria Lewis Kussmaul</td>
<td>Co-Founder and Partner, ACG Partners</td>
</tr>
<tr>
<td>Aaron Mackey</td>
<td>Frank Stanton Legal Fellow, Electronic Frontier Foundation</td>
</tr>
<tr>
<td>David Mahon</td>
<td>Chief Security Officer, CenturyLink, Inc.</td>
</tr>
<tr>
<td>Dr. Doug Maughan</td>
<td>Director, Cyber Security Division, DHS Science &amp; Technology Directorate</td>
</tr>
<tr>
<td>Randy Miskanic</td>
<td>Chief Information Security Officer and Vice President Digital Solutions, U.S. Postal Service</td>
</tr>
</tbody>
</table>
JOEL MOLINOFF  
Senior Vice President  
Chief Information Security Officer  
CBS Corporation

CHRIS MORGAN  
Co-Founder and President  
IKANOW

VALMIKI MUKHERJEE  
Chairman & Founder  
Cyber Future Foundation & Constituants

DR. SRINIVAS MUKKAMALA  
CEO  
RiskSense

ERIK NAUGLE  
Director of Cloud and Internal Hosting Security  
Intuit

HUGH NJEMANZE  
Founder and Chief Executive Officer  
Anomali

RICK ORLOFF  
Chief Security Officer  
Code 42

LOUIS PARKS  
President & CEO  
SecureRF Corporation

PHIL QUADE  
Special Assistant to Director NSA for Cyber  
Chief of NSA  
National Security Agency

MICHAEL RAGGO  
Director of Security Research  
MobileIron Security Labs (MISL)

PHILIP R. REITINGER  
President and Chief Executive Officer  
Global Cyber Alliance

DAN ROAM  
President  
Digital Roam Inc.

RICHARD RUSHING  
Chief Information Security Officer  
Motorola Mobility LLC

ENRIQUE SALEM  
Managing Director  
Bain Capital Ventures
SINET Mission
SINET Mission

Advance innovation and enable global collaboration between the public and private sectors to defeat Cybersecurity threats.

ABOUT SINET

SINET is a “super connector.” We provide a series of platforms for the business of Cybersecurity to take place within the global ecosystem of the entrepreneur including venture capital, investment banking, system integration, academia, science, legal, policy, and industry as well as Government intelligence, military and civilian departments and agencies.

Our programs consistently attract the highest level of international industry and government executives. SINET is well known for our coveted and unparalleled networking opportunities.

Learn more at www.security-innovation.org

COMMUNITY BUILDING

SINET—where the business of Cybersecurity takes place—builds communities of interest and trust, connects thought leaders in government and industry with builders, buyers, researchers and investors across the international security domain with the goal of promoting and advancing Cybersecurity innovation. We are passionate about our mission and strive to build a community that engenders a sense of common duty, purpose and commitment to protect our critical infrastructure and help to preserve economic stability.

Join our community and participate in our mutually beneficial, trust-based approach that connects the ecosystem of the entrepreneur, increases business opportunities and advances Cybersecurity innovation.

Join the SINET community at www.security-innovation.org/community.htm

MEMBERSHIP

The IT Security Entrepreneurs Forum (ITSEF) is just one of the many resources available to the SINET community. By becoming a member, you will gain access to additional benefits and discounted services that can take your company to the next level. Many of your peers have already discovered that SINET is the Cybersecurity “super connector” that enables them to exchange knowledge, learn from industry experts, advance innovation, and build networks with investors, entrepreneurs, government agencies, military, corporate enterprises and more.

Together, we can make a difference. Become a SINET member and help contribute to our mission of advancing the business of Cyber.

To learn more about membership contact Janice Mawson at membership@security-innovation.org
Upcoming SINET Programs

Supported by The US Department of Homeland Security Science & Technology Directorate
Upcoming SINET Programs

**Innovation Summit 2016—New York, NY**
“Connecting Wall Street, Silicon Valley and the Beltway”
July 14, 2016
The TimesCenter

Innovation Summit connects America’s three most powerful epicenters—Wall Street, Silicon Valley and Washington, DC—and promotes the importance of industry and government collaboration. The summit is designed to reinvigorate public-private partnership efforts between disparate communities and accelerate the business of Cybersecurity between investors, builders and buyers.

**SINET61 2016—Sydney, Australia—New International Offering**
Supported by Data61
September 13 & 14, 2016
Australian Technology Park

SINET61 fosters the Australian national Cyber priorities in a global context by connecting London, Washington DC, New York City, Silicon Valley, Sydney, the Asia Pacific region and other centers of innovation.

**Showcase 2016—Washington D.C.**
“Highlighting and Advancing Innovation”
November 2 & 3, 2016
The National Press Club

SINET Showcase provides a platform to identify and highlight “best-of-class” security companies that are addressing industry and government’s most pressing needs and requirements. The chosen SINET 16 Innovators present their technological solutions to representatives from the ecosystem of the entrepreneur: venture capital, investment banking, system integration, academia, science, legal, policy, private industry and executives from the Federal Government, including civilian, intelligence and military professionals. Showcase’s objective is to increase awareness of innovative solutions that may lead to an investment in, or the purchase of, advanced technologies that will help secure our nation’s critical infrastructure and command-and-control systems.

**SINET presents**
**The Global Cybersecurity Innovation Summit 2017**
May 2017
The British Museum, London

The Global Cybersecurity Innovation Summit objective is to advance innovation and the growth of the Cybersecurity sector by providing a platform for Cybersecurity businesses, particularly Small and Medium Enterprises (SMEs), to connect with key UK, US, and International decision makers, system integrators, investors, Government policy makers, academia and other influential business executives. Last year’s event sold out. Register early to secure your spot.
SINET Members
SINET Members
MEMBERS