2016 FS-ISAC Fall Summit

STRENGTH IN SHARING
expanding the trust

Nashville, TN · Gaylord Opryland · October 23 - 26
On behalf of FS-ISAC and the 2016 Fall Summit Planning Committee, I am pleased to welcome you to the 2016 FS-ISAC Fall Summit.

As Partners in the Information Security community we have all been challenged in 2016 with the onslaught of DDoS and phishing campaigns with payloads that have included credential stealing malware, destructive malware and ransomware. In addition, to the evolving threat landscape, we are challenged with supporting our corporate strategies that look to leverage advancing technology and services that expand our perimeter boundaries and place a greater demand for protecting the information that our customers and fellow employees entrust us with. From a governance perspective we are seeing increased government and industry regulations and our corporate boards are demanding greater visibility into our programs. These challenges are expanding the responsibilities placed upon us as security professionals and requiring us to ensure we are following best practices.

In the dynamic environment that we all work in today, the best practices that are effective today may not be effective tomorrow. Having the latest information on threats, sharing of best practices and trends across our sector has become more important than ever. FS-ISAC plays a vital role in making that happen. Because there is “Strength in Sharing,” FS-ISAC continues to push the envelope when it comes to gathering reliable and timely information from financial services providers, commercial security firms, federal/national, state and local government agencies, and other trusted resources and disseminating that information globally. They have set a high standard for themselves when it comes to the quality of the information they share, the access to trusted partners they provide and the content they deliver through their annual conference.

If you have joined us at previous events, you already know that the FS-ISAC conferences offer excellent, content, amazing venues, industry leaders and guest speakers. This year’s Fall Summit, to be held at the Gaylord Opryland Hotel, once again aims to exceed your expectations with content covering governance, data protection, threat intelligence and cyber-attacks. The FS-ISAC is also delighted to have as keynote Schwartz Senior Fellow and CNN Terrorism Analyst Peter Bergen.

Whether you are representing a global bank, community institution, large or small insurance company or any company in the financial services sector, we all have a common goal and that is to protect our company brand and the data that has been entrusted to us. Come join us as there is “Strength in Sharing.”

I look forward to personally welcoming you in Nashville this October.

Bill Downes, CISSP
Chief Information Security Officer
The Hartford
Conference Chair, 2016 FS-ISAC Fall Summit
Who Should Attend?
- CEO, CISO, CSO, CIO, CTO, and CRO
- Head of Threat Intelligence
- EVP, SVP, VP, and Director of these areas:
  - Security Operations
  - Business Continuity
  - Fraud
  - Audit and Compliance
  - Investigations
  - Payment Risk Management
  - Physical Security
  - Payment Operations
- Payment Line of Business Managers including:
  - Online Banking
  - Online Treasury Management

Why You Should Attend
- Presentations by over three dozen senior executive FS-ISAC members
- Concrete take-aways including case studies and best practices
- Interactive sessions that allow for strategic and solution-oriented discussion
- Actionable information and sharing designed specifically for financial services institutions
- Complimentary attendance for Premier and above members
- All meals and events during the conference are included

Attendance Restrictions
The 2016 FS-ISAC Fall Summit restricts attendance to regulated financial services firms, relevant public sector entities, and country-level banking associations and payments associations. Examiners and those responsible for informing public policy are not eligible to attend. If you have questions regarding eligibility, contact marketing@fsisac.com.

FS-ISAC Premier, Gold and Platinum Members receive complimentary registration passes as follows below. After all complimentary passes are utilized, additional member firm staff may attend at the Standard Member Registration rate below.
- Platinum members receive ten (10) complimentary passes
- Gold members receive five (5) complimentary passes
- Premier members receive two (2) complimentary passes

<table>
<thead>
<tr>
<th>FS-ISAC Affiliation</th>
<th>Early Bird (ends 9/23)</th>
<th>Standard Registration (after 9/23)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platinum/Gold/Premier Member</td>
<td>COMPLIMENTARY</td>
<td>COMPLIMENTARY</td>
</tr>
<tr>
<td>Standard Member</td>
<td>$795</td>
<td>$1,250</td>
</tr>
<tr>
<td>Basic/Core Member</td>
<td>$895</td>
<td>$1,500</td>
</tr>
<tr>
<td>CNOP (Critical Notification Only Participant)</td>
<td>$895</td>
<td>$1,750</td>
</tr>
<tr>
<td>Government</td>
<td>$895</td>
<td>$895</td>
</tr>
<tr>
<td>Non-Member (eligible FI only)</td>
<td>$895</td>
<td>$1,750</td>
</tr>
<tr>
<td>Guest*</td>
<td>$895</td>
<td>$895</td>
</tr>
<tr>
<td>Monday Grand Ole Opry Dinner Event Guest**</td>
<td>$159</td>
<td>$159</td>
</tr>
</tbody>
</table>

* Guest registration may include spouse, family members, significant others, etc., but does not apply to colleagues or other practitioners in the financial services community. Guests do not attend sessions, but only meals and networking events.
** "Monday Grand Ole Opry Dinner Event Guest" registration includes spouse, family members, significant others, etc, and only includes access to the Monday Dinner event from 7-11pm at the Grand Ole Opry. This registration will not grant access into any other portion of the event. This is not to be used by sponsor firms to send additional representatives to the dinner event.

Conference Registration Cancellation
Cancellations received prior to September 19 will not be subject to a cancellation fee. Cancellations received on or after September 19 will be subject to a $200 USD cancellation fee. This applies to all members at all tiers as well as Non-Member, Guest, Government, CNOP, and BITS member registration regardless of registration fee paid. Any member/non-member cancellations must be received via email to summit@fsisac.com. Registrations are transferable within an organization without penalty.

Online Registration
www.fsisac-summit.com/fall-attendee-registration
The FS-ISAC has reserved a block of rooms at the Gaylord Opryland at a group rate of $199 per night (plus tax). Please make your reservation as soon as possible, as this block will fill quickly. The hotel reservation cut-off date is October 1. To make your reservation, please call the reservation line listed above or visit www.fsisac-summit.com/fall-hotel-travel. Please be sure to mention that you are with the 2016 FS-ISAC Fall Summit to receive the group rate.

Airport and Transportation
Nashville International Airport (BNA) - 8.3 mi (approximately $30 USD taxi)

Pricing
On-site overnight parking fee: $24 USD daily
Valet parking fee: $32 USD daily

Peter Bergen
Presenting: Making Sense in a World of Trouble

FS-ISAC is excited to have Peter Bergen as the 2016 FS-ISAC Fall Summit Keynote speaker. Bergen is a Schwartz Senior Fellow at the New America Foundation in Washington D.C.; an Adjunct Professor at the School of Advanced International Studies at Johns Hopkins University; CNN’s terrorism analyst and author of Holy War, Inc.: Inside the Secret World of Bin Laden (Free Press, 2001). Holy War, Inc. was a New York Times bestseller and has been translated into eighteen languages. A documentary based on Holy War, Inc., which aired on National Geographic television, was nominated for an Emmy in the research category.
2017 Global State of Information Security Survey - Highlights and Trends in the Financial Services Industry | The presenting company will preview their 2017 Global State of Information Security Survey results and highlight trends in Financial Services. The results are typically made public in October, and they will showcase them during this session.

CAPS 2016 Reports | FS-ISAC CAPS exercises are one of the largest table top cyber threat exercises in the industry. The session will report on the aggregate results of more than 1,000 North American incident response teams’ answers to the September 2016 exercise testing destructive malware attacks to wholesale payment operations.

Changing User Behavior – Going Beyond Traditional Training and Awareness | Historically, attempts at changing behavior have primarily been limited to either influencing through training and awareness, or an outright blocking of the capability. The presenting company has implemented a program, entitled Adaptive Enablement, that goes beyond these traditional methods and influences behavioral changes using a combination of new techniques and tools. This session will review those techniques and the real world results they have produced.

CISO Case Study: Gaining Continuous, Data-driven Visibility into Cyber Risk and Security Control Performance | The presenters will discuss how security leaders can harness data science and big data technology to advance, simplify and automate the way they:

- Identify, measure and communicate material risk to Executives
- Show the value of security investment and justify priorities to protect critical assets
- Maximise the time their team have to focus on security, rather than battling with PowerPoint and Excel
- Ensure GRC stakeholders have the tailored information they need, when they need it

Attendees will hear practical examples of opportunities, challenges (both business and technical) and how to solve them.

CISO Panel: Structuring a Successful Information Security Organization | Information Security organizations have changed dramatically over time, driven by the changes in threats, attacks, technology and business requirements. What roles do CISO’s see as essential to the success of the organization and firm, what skills are needed, and what tools enhance the organizations ability to protect the enterprise.

CISO Panel: The First 100 Days of Being a CISO | When you start the first day in the CISO role, the challenges can seem daunting. Assessing the organization and people, as well as understanding the existing controls and issues (and the gaps) are important steps. Listen to a panel of successful CISOs as they discuss their experiences in getting started in the role.

Cognition and the Future of Security | Security teams face an onslaught of serious challenges that are impossible to keep up with such as skills shortage, volumes of data, and an evolving security landscape. A tremendous amount of security knowledge is created for human consumption but it is mostly untapped. The company is bridging the gap and unlocking a new partnership between security analysts and technology with the world’s first cognitive analytics solution using core Watson technology to understand, reason, and learn about security topics and threats. Attend this session to learn how they are revolutionizing the way security analysts work by using cognitive security to gain powerful insights, reduce threat research, and save time and money.

Completing the Risk Equation by Integrating Threat Intelligence into VM Processes | There is an urgent need for industry-wide standardization to give IT security teams the ability to share threat intelligence data, leverage that data to significantly reduce security data overload, and quickly and effectively manage the right risks at the right time. By integrating threat intelligence into vulnerability risk management processes, testers and remediators can move beyond CVSS to identify and mitigate their most critical risks based on situational business context rather generalized ‘high,’ ‘medium,’ and ‘low’ rankings. Using standardized threat intelligence formats (STIX and Cybox) and common languages (JSON, XML, and API), companies can make better security decisions and utilize their limited resources to fix vulnerabilities that pose the highest risk to their company and their clients.
Crowdsourcing Solutions Forum with Members | Have a tricky problem that you want to know how other member companies are addressing? Bring your issue to the Crowdsourcing Solutions Forum. This session will focus on industry members and the FS-ISAC staff sharing approaches to solving or addressing tricky problems. To get the discussion started, we will either ask for an audience topic or pull from the list of FS-ISAC surveys. The more the audience participates, the longer the discussion will be on each topic.

Cyber Security in the Cloud – It’s Safer Up There! | Moving to the cloud is being increasingly relied on as a vehicle for agile, scalable and elastic solutions, and today’s leaders are building competitive advantage and cutting costs by leveraging cloud capabilities. However, a 2016 survey by Clutch indicated that almost 75% of respondents felt that the cloud was not much more secure than legacy systems, fueling the concern that overshadows cloud adoption. This panel will discuss not only the performance benefits of the cloud, but also the security benefits which can provide a much stronger defense than on-premise systems.

Defining the Core Security and Compliance Requirements for Office 365 | Almost every company has deployed, is in the process of deploying, or is considering deploying Office 365 (O365). And while Microsoft is laser-focused on driving utilization, InfoSec teams are now responsible for protecting sensitive data in OneDrive, Exchange, SharePoint Online, and Yammer. This panel will ask three IT Security leaders what their core security and compliance requirements are for O365 and how they are planning to support them.

Delivering Secure Solutions in Agile Cultures | The values of agile cultures are not in opposition to information security. The burden to achieve security within agile requires changes in approach, culture and tooling. Move to market faster, lowering solution overhead and raise the level of security in your environment.

Early Breach Warning: Using Intelligence Driven Fraud Analytics to Stop Fraud | The diversity of available payment types has led to an increase in cybercriminals evolving how they exploit payment systems. Building on a talk given at the Fall 2015 and Annual 2016 Summits, this talk explores how intelligence gleaned from the Darkweb can be combined with big data analytics to identify compromised merchants more quickly than previous methods and lead to proactive measures to stop payment card fraud before it occurs. This session will also explore how the “liability shift” has affected the industry one year after implementation.

Establishing a Risk Management Program for Your Small to Midsize Institution | Existing and emerging risks antagonize institutions daily. Having effective risk assessment and management is critical in identifying and mitigating risk. This session provides small to midsize institutions with the appropriate direction to stand up a program to effectively manage IT risks and demonstrate compliance to regulators. Using best practices, attendees will learn how to create or improve upon their own risk management processes.

Heart Attacks vs. Headaches: Balancing Security and Business | Security teams are tasked with keeping organizations safe from cyberattacks. However, organizations are often forced to choose between security and business needs. This is an impossible dilemma, and nowhere is this more apparent than with endpoint security. Not only do we as an industry struggle to protect our users, but the solutions and policies we implement are often so obtrusive that we end up causing more frustration than anything else.

It is time to reverse this trend. In this session, attendees will learn about the following:

- Impact of endpoint security on workforce productivity
- Common endpoint security mistakes
- The most damaging endpoint blind spots
- Recommended approaches that have been proven to work

How Converging Identity Management and GRC Capabilities Have Helped Us Stay Ahead of the Cybersecurity Curve | A world renowned Chief Security Officer and a GRC National Managing Partner share their lessons learned in converging IAM and GRC capabilities to help them stay ahead of the cybersecurity curve. Learn how building a service-oriented security organization, and breaking down barriers between physical and cybersecurity, banks can better address advanced threats and attacks, provide management more meaningful metrics and analytics for decision making – all enabled through an integrated risk and compliance solution.
It’s Time to Move Beyond CTI: Business Risk Intelligence | This panel will discuss what needs to happen to “Make Threat Intelligence Great” again. This will entail focusing on “Business Threat Intelligence” that works with other teams away from cyber security such as Fraud/Physical/Supply Chain. They will discuss examples of real life cases where threat intelligence has led to impacting business and away from reporting on hashes and indicators.

Leveraging Threat Intelligence (Public and Private) for Small to Mid-Sized FIs | This panel will involve small to mid-sized financial institutions sharing their successes in utilizing threat intelligence and automation. One of the biggest struggles for smaller institutions is consuming intelligence and activating it in the defense of their infrastructure and digital assets. FS-ISAC has largely helped provide a stream of intelligence, but how does an institution take the next step? This panel will look at the human resources aspects (dedicated vs. shared roles in IT for security), technologies implementations (punch++, FS-ISAC/Soltra, STIX, etc.), as well as the financial investments required behind such a program.

Managing Endpoint Security Baselines with Group Policy | Group policy is an often misunderstood and underutilized baseline configuration management tool within the Microsoft Windows arsenal. Institutions will learn how they can leverage this tool to learn how to best assess and apply recommended security settings to the Windows operating system using tools you likely already own tools. If you are interested in learning how to manage your fleet with baseline configuration management practices, then you should attend this talk.

Mitigating APT Lateral Movement with Cyber Deception | This session will look in-depth at cyber deception, considered by Gartner to be an upcoming trend. When an APT attack is successful, the threat actors “pivot” and perform lateral movement, attempting to reach other endpoints and servers on the network. This allows those attacked to control the movement and mitigate the attacker who has bypassed all other APT countering controls. The speaker will discuss the current asymmetry of cyber defense, cyber deception theory, technology, implementation considerations, value, and use cases to display how lateral movement can become an economic hurdle for attackers.

Nuisance to Nefarious Threat – Shielding Your Organization from the Ransomware Epidemic | Ransomware used to be more of a consumer or end-user problem. Now criminal groups have evolved their methods into a big business, infiltrating Ransomware into networks and effectively repurposing those networks to monetize your data against you. They have grown so complex and varied that traditional IT system defenses such as antivirus (AV) software and intrusion prevention systems (IPSs) are not enough on their own. This session will delve into the nefarious and sophisticated evolution of Ransomware, highlighting the details that could be key to keeping your organization safe. Attendees will understand how to apply additional layered security and maintain specialized visibility into these attacks. They will also hear three ways to reduce and manage operational risk in the face of this evolving cyber-threat.

Practical Solutions for Managing Access and Assets | The financial industry is faced with many pressing cybersecurity challenges, including how to manage IT assets and access rights. You can’t protect what you don’t know you have nor ensure staff has the appropriate level of access if you don’t know what rights they have. This session will provide an overview of the NCCoE and describe two projects that FS-ISAC members identified as significant challenges. The first project outlines a practical solution for identifying and managing IT assets within an organization. The second, Access Rights Management, addresses how to integrate diverse identity and access management platforms to better control access rights. These projects were initiated through discussions with FS-ISAC members and have broad applicability across the financial sector.

Preparing For A Bad Day Through Cyber Exercises | A panel will discuss what several banks have done and are doing when it comes to preparing their technical and executive staff through the implementation of cyber threat-based exercises. They will consist of five major banks that have started internal cyber exercise programs/teams to plan and conduct exercises: BoA, JPMC, AMEX, and Regions, with Citi as moderator. They will discuss how teams are composed, missions, basic exercise types, structures, remediate identified shortfalls/gaps.

Priming the Board for Cybersecurity | The bar has been set for the Board of Directors to manage cyber security risk. Practical ideas on how to do the limbo with the Board!

Putting The OPSEC In OpIntel: A Proposal for Sharing Operational Intelligence | Targeted malware and payloads often contain artifacts unique to a given enterprise, such as hardcoded credentials to support lateral movement.
As important as it is to identify these threats, sharing plain text passwords/credentials with a hunt capability/service could be a non-starter for an organization. The speakers will propose a system for achieving this operational intelligence capability, via a publish/subscribe model, while still ensuring that the plaintext version of artifacts of “interest” to an organization (e.g. password strings, unique host names, etc.) remain unexposed to the system.

Ransomware - An Educated Response | Throwing money at a problem doesn’t make it go away. Social engineering methods and the “evil genius” cyber criminals behind the attacks are furiously innovating, keeping IT off-guard. Ransomware continues to proliferate and evolve with new hybrid attacks despite the best efforts of endpoint security and gateway solutions to block them. How do you keep up and what are the most effective methods for securing your organization to combat cyber crime? This presentation will cover how financial institutions can stay ahead of social engineering traps and lower risk.

Ransomware Driving Hacker Innovation – The Evolution of Cryptowall | Ransomware has become a constant threat to users. Initially targeting through spam campaigns, Cryptowall has evolved into an advanced piece of malware that is now usually delivered through the Angler exploit kit. Working with Limestone Networks, Talos was able to determine that Angler dropping Cryptowall is generating over $30 million a year, which has enabled Angler and Cryptowall to constantly evolve and innovate. This talk will show how Cryptowall evolved from a spam based attack in Version 2 to an exploit kit payload in Version 4. It will also show how the rise in effectiveness of Cryptowall has led to a constant stream of innovation in the features incorporated into the Angler exploit kit.

Reducing Your Attack Surface: Detect and Manage Web Components, 3rd Party Software and Shadow IT | What if you could find common elements used across the internet that increase your risk of a breach and eradicate them from your internet facing assets? This session will demonstrate how to leverage vulnerable web components within applications, third-party software with security holes, and risky services being used by your employees and users. By traversing these markers and finding where they exist across your external web facing infrastructure, you can dramatically reduce your attack surface and eliminate some common threat vectors used by hackers.

Re-Thinking Perimeter Security - Why Leading Banks Are Moving To Security-as-a-Service | Traditionally, financial services companies have adopted best of breed appliances with associated maintenance and consulting services for perimeter security. The current on-premise perimeter security architecture is being overtaken by a “Security-as-a-Service” provider model. Devices you do not own or trust are connecting to corporate owned data and applications running both in the cloud and within on-site data centers creating a need to re-architect network defense and policy management. The speaker will be joined by a top tier financial services firm to describe how this approach addressed the new requirements introduced by BYOD, Cloud, Social, and Mobile. They will lay out the challenges effecting the bank, the adoption plan and a path to a successful deployment, followed by sharing the benefits realized since adopting the cloud.

Security 101 - Basics of a Security Program | This session will provide the attendees with a framework upon which they can determine the elements of a security program that they need to put into place in their operations. The session will illustrate how the NIST Cybersecurity Framework could be used as a foundation for building their program and ensuring that they have the right components in place. Terminology will be defined and illustrated throughout the presentation.

Software Defined Security | This session will introduce the concept of software defined security with the use of Critical Stack to rapidly develop and deploy security solutions within an organization. Learn how to reduce the reliance on security vendors, build a community to solve complex security problems faced by Financial Institutions, and collaborate on a platform that allows easy adoption and deployment of open source solutions.

Solving Critical Problems With Big Data Analytics | This session features three rapid-fire presentations highlighting how big data analytics can solve critical security concerns in the financial services industry. A security analytics expert will kick things off with an overview of how advances in User and Entity Behavior Analytics (UEBA) enable threat prediction, prevention and detection capabilities that are transforming information security. They will be followed by industry-leading CISOs who will share how they are using big data-driven solutions to insider threats and trade surveillance.
The Challenges of InfoSec Leadership in Community Banking | This session will feature a dynamic, moderated panel discussing common information security leadership strategies, techniques, and ideas to solve the unique problems that community institutions face, from the boardroom to the frontlines. What works? What doesn’t? What can the industry do better? Audience participation is highly encouraged - nay, expected, to further the collaborative and sharing ideals of FS-ISAC. Give us your nuggets of wisdom, your experiences, and let’s learn from each other!

The Latest DDoS Attack Trends and DDoS Defense Best Practices for Financial Organizations | DDoS Extortion attacks and DDoS attacks used as a smokescreen to cover up non-authorized data exfiltration or fraudulent wire transfers are just some of the DDoS attack trends threatening financial institutions. There is little doubt that DDoS attacks continue to rise in size, frequency and complexity, but what is becoming more apparent is the close interrelationship between DDoS attacks, other forms of malware, and how they can be used together during advanced threat campaigns against your organization. In this session, the speaker will present the latest in DDoS attacks trends, best practices in DDoS attack defense, and some interesting results from the latest FS-ISAC Survey on DDoS Mitigation Strategy.

The Myth of Phishing Awareness | People click phishing emails because they are unaware of the threat. So the answer is to make them aware right? Early on I believed this too, until the data proved it completely wrong. In 2008 this was partly true, in 2016, we need to bury this fairy-tale.

There be Dragons in my MDM! Effectively Deploying Data Protection Technology in a Master Data Mart | The lifeblood of financial services is data. This data has an extremely complex set of interactions with software and hardware. MDM hub is growing in popularity as an effective approach to manage the master data that is stored in databases, and to keep it synchronized with the transactional systems that use it.

Join this session to learn more on effective data security according to a hypothetical Business Case. Topics to be covered include:

- Implementing a MDM hub to consume all customer data system of record feeds “silver data”): logic, tool sets, personas and levels of access
- Standard Security Requirements: “Walled Garden”, Access Logging & Auditing, Hundreds of roles and access control levels, diverse views, Data in transit requirements
- Encryption: Not your father’s encryption solution, Gradual approach, one data element at a time, Ever increasing circles of risk reduction, Field-based access control, Reduction of need for compensating controls

The Rising Tide of Cybercrime: How to Keep Our Head Above Water | There is little reason to be optimistic about the future of information security. An overwhelming majority of those surveyed at the 2016 FS-ISAC Annual Summit said they expect the pace of cyber-attacks to increase over the next five years. Awash in a sea of sophisticated threats, many organizations question whether they can keep their head above water. In this panel, experienced security professionals examine today’s trends in cyber-attacks, including the resurgence of ransomware, and the risks that are making the cybersecurity industry so challenging to navigate. Panelists will debate why there may—or may not—be hope for a more secure future, and what actions organizations can take to more effectively prevent, detect, and respond to this rising tide of cybercrime.

Wire Fraud: Dealing with Wire Fraudsters and Mules | CEO/CFO targeted wire fraud is an ongoing threat with losses to banks of all sizes. However, if the initial fraudulent request is recognized and intercepted, then it is possible to play the fraudster(s) and shut down the accounts they use. By playing along and contacting the compromised banks, industry experts can shut down valuable assets used by the fraudsters losing them money and time as well as saving banks from losses. It is time the good guys pushed back and this is a fun and easy method to do so that also saves banks from unnecessary losses.

You Might be a Community Bank but You Are Still a Target | Many community banks have traditionally managed cyber security in-house, but now recognize the costs and resources needed to do so properly. Come learn how this speaker is leveraging outsourced services for quick, resilient access to cyber defense tools and expertise associated with the larger banks. Key stops to future proofing internal cyber security to address upcoming regulatory compliance initiatives will also be shared.
Silver Solutions Showcase*
Join us for complimentary snacks and refreshments, and a technology showcase where the latest technical innovations in cyber-awareness, proactive security, and defense will be on display. In this relaxed setting, attendees may select up to three solutions they would like to see. These information-packed 15-minute sessions will be presented by technology experts from our solution providers, be use-case driven, and tailored to the unique needs of FS-ISAC members.

- Keeping the Customer First: Considerations for Successful Digital Transformation | Akamai
- Unburdening Threat Hunters by Operationalizing Threat Intelligence Data | Anomali
- The Art and Science of Deception for Empowering Response Actions and Threat Intelligence | Attivo Networks
- Use MX Record Monitoring to Put the Brakes on BEC/Social Engineered Email Attacks | BrandProtect
- Talking to Your Board of Directors About Cyber Risk | Coalfire
- Cybersecurity Strategies Require Privilege Account Security at the Core | CyberArk
- The Untold Secrets for Fighting APTs | Cybereason
- Beyond Threat Detection and Takedown: Prediction, Analytics and Deterrence | Easy Solutions
- Achieving ‘Left of Boom’ through the Hunt | Endgame
- A Proactive Approach to Mitigating Risk, Ensuring Compliance to Information Governance | Guidance Software
- The Root of Modern Threats: Misuse and Compromise of Identity | Gurucul
- A Journey Through the Dark Matter of Your Network | illusive networks
- Data Science Use Cases for Cyberattack Detection and Prevention | Interset
- The Hidden Enemy: Malvertising and Ransomware | Malwarebytes
- Eliminate Malware with Menlo Security’s Isolation Platform | Menlo Security
- Netskope: Cloud Application Security for All Use Cases | Netskope
- Are You Focused on the Threats that Matter? | NSS Labs
- Identity Centric Security...It is Everywhere! | Optiv
- 3 Critical Threat Intelligence Use Cases For Your Organization | Recorded Future
- Modernize Your 3rd Party Risk Management Process | RiskRecon
- Security Ratings & Continuous Risk Monitoring | SecurityScorecard
- Trusted Hackers Who Want To Be Your Allies, Not Your Adversaries | Synack
- Signoff or Sign-Out | Synopsys
- You Have a Blind Spot – Exposing The Misuse of The Foundation of Online Security | Venafi

Innovative Technology Showcase
You will want to make sure to add this showcase to your schedule in Nashville. The Innovative Technology Showcase sessions are not product or sales pitches but short, bite-sized discussions around industry related topics, issues and interests. Designed to be similar to TED Talks, these eight-minute sessions offer an unique experience to hear expert dialogue from vetted and approved sponsors.

- Don’t Fly Blind into the Container Storm | Aqua Security
- Unique Mobile Threat Defense Technology That Predicts and Protects Against Advanced Cyber Attacks | Skycure
- Internet 101: The 5 Facts You Keep Forgetting | The Media Trust
- Hack Yourself First: A Risk Based Approach to Application Security | Whitehat Security
Sunday, October 23
4:00 - 7:00 pm  Early Registration
5:30 - 7:00 pm  Opening Welcome Reception
7:15 - 9:00 pm  Sponsored Member Dinners*

Monday, October 24
7:30 am - 7:00 pm  Member Registration
7:30 - 8:30 am  Board and Member Breakfast*
8:30 - 10:00 am  Board Meeting*
8:30 am - 12:30 pm  Members Only Technical Forum*
12:30 - 1:30 pm  Birds of a Feather Lunch*
1:30 - 5:00 pm  Members Only Meeting*
3:00 - 6:00 pm  Sponsor Registration and Sponsor Hall Set-up
5:00 - 6:00 pm  Solutions Showcase*
6:00 - 7:00 pm  Networking Reception in Sponsor Hall
7:00 - 9:00 pm  Grand Ole Opry Dinner Event
9:00 - 11:00 pm  After Hours Hospitality Event

Tuesday, October 25
7:00 am - 7:00 pm  Registration
7:00 - 8:00 am  Breakfast
8:00 - 8:15 am  Opening Remarks
8:15 - 9:15 am  Keynote Session
9:15 - 9:45 am  General Session
9:45 - 10:15 am  General Session
10:15 - 11:00 am  Networking Break in Sponsor Hall
11:00 am - 12:00 pm  Concurrent Breakouts
12:00 - 1:00 pm  Lunch
12:00 - 1:00 pm  FS-ISAC 101
1:00 - 2:00 pm  Concurrent Breakouts
2:00 - 2:30 pm  Networking Break in Sponsor Hall
2:30 - 3:30 pm  Concurrent Breakouts
3:45 - 4:45 pm  Concurrent Breakouts
5:00 - 6:00 pm  Solutions Showcase*
6:00 - 7:30 pm  Networking Reception in Sponsor Hall
7:30 pm  Sponsor Dine Around

Wednesday, October 26
7:00 am - 6:00 pm  Registration
7:00 - 8:00 am  Breakfast
8:00 - 8:15 am  Opening Remarks
8:15 - 9:00 am  General Session
9:00 - 9:30 am  General Session
9:30 - 10:00 am  Networking Break in Sponsor Hall
10:00 - 11:00 am  Concurrent Breakouts
11:15 am - 12:15 pm  Concurrent Breakouts
12:15 - 1:15 pm  Lunch
12:15 - 1:15 pm  Innovative Technology Showcases
1:30 - 2:30 pm  Concurrent Breakouts
2:30 - 3:00 pm  Networking Break in Sponsor Hall
3:00 - 4:00 pm  Solutions Showcase*
3:00 - 5:00 pm  Sponsor Hall Tear-down
4:15 - 5:00 pm  General Session
5:00 - 6:00 pm  Closing Remarks and Reception
6:00 - 9:00 pm  Sponsored Member Dinners*

*closed to Sponsor Attendees with the exception of companies sponsoring at this event
2016 FS-ISAC Fall Summit

STRENGTH IN SHARING
expanding the trust

Nashville, TN · Gaylord Opryland · October 23 - 26

SOLTRA

www.fsisac.com | www.fsisac-summit.com

GOLD SPONSORS