2017 FS-ISAC FALL SUMMIT

STRENGTH IN SHARING


Baltimore Marriott Waterfront
1-4 October
WHO SHOULD ATTEND?
- CEO/Bank Owners, CISO, CSO, CIO, CTO and CRO
- Head of Threat Intelligence
- EVP, SVP, VP and Director of these areas:
  - Security Operations
  - Fraud and Cybercrime
  - Investigations
  - Physical and Information Security
- Business Continuity
- Audit and Compliance
- Payment and Security Risk Management
- Payment Operations
- Payment Line of Business Managers including:
  - Online Banking
  - Online Treasury Management

NEW THIS YEAR
- Sunday afternoon pre-trainings
- National Cyber Security Alliance (NSCA) training for small/medium business
- Innovation challenge/competition
- ‘Capture the Flag’ interactive event
- Sunday welcome reception and game night

MEMBER SESSIONS
- More member presented sessions than ever before
- HOT TOPICS! Session on hot topics, selected by attendees, just before the start of the event
FS-ISAC is pleased to welcome you to the 2017 FS-ISAC Fall Summit. As partners in the information security community, we have all been challenged with issues this year including:

1. Increasing malware campaigns, including ransomware
2. Overwhelming volumes of complex threat intelligence
3. Increasing governance and regulation
4. Rise in political hacktivism
5. Greater demands for metrics and reporting

As a whole, we are challenged with protecting our current environments while preparing for future changes in technology and malware. We must adjust to changing and increasing regulations, while supporting internal corporate strategies that are more frequently adopting technology that pushes beyond our traditional perimeters and models. These challenges expand the responsibilities placed upon us in security industry and as individual professionals. Meeting these challenges requires us to come together as a community and ensure we are following best practices. Unfortunately, in the dynamic environment in which we work today, 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. Access to high quality information and trusted partners is crucial.

If you have joined us at previous events, you already know that FS-ISAC Summits offer excellent, content, amazing venues, industry leaders and guest speakers. This year’s Fall Summit, to be held at the Baltimore Marriott Waterfront, once again aims to exceed your expectations with content covering governance, data protection, technology trends, threat intelligence and cyber-attacks. We are excited about our keynote speaker John Brennan who recently served as director of the Central Intelligence Agency. As CIA Director, Brennan managed U.S. intelligence collection, analysis, covert action, counterintelligence and liaison relationships with foreign intelligence services.

All financial institutions have a common goal to protect our customers, company brand and the data that has been entrusted to us. Come join us as there is “Strength in Sharing”.

FS-ISAC
ATTENDANCE RESTRICTIONS

The FS-ISAC Fall Summit restricts attendance to regulated financial services firms, relevant public sector entities, and country-level banking associations, payments associations and LS-ISAO Members. Examiners and those responsible for informing public policy are not eligible to attend. If you have questions regarding eligibility, contact marketing@fsisac.com. If you are a solutions provider, please visit fsisac-summit.com/2017-Fall-Sponsorships.

Payment is required at the time of registration. If you require an invoice, please contact admin@fsisac.com.

FS-ISAC PREMIER, GOLD AND PLATINUM MEMBERS

If you would like to utilize one of your companies limited complimentary passes, please reach out to your company Point of Contact with FS-ISAC to obtain a limited complimentary coupon code. Coupon codes must be used at point of purchase. If you have any questions on who your point of contact is, please contact admin@fsisac.com. All additional Premier, Gold and Platinum members above the complimentary amount will be subject to the Member registration fee outlined below.

Deadline to register complimentary registrations is 31 August.

PREMIER Member - two (2) complimentary full-Summit passes
GOLD Member - five (5) complimentary full-Summit passes
PLATINUM Member - 10 complimentary full-Summit passes

<table>
<thead>
<tr>
<th>FS-ISAC Affiliation</th>
<th>Early Bird (ends 25 August)</th>
<th>Standard Registration (after 25 August)</th>
</tr>
</thead>
<tbody>
<tr>
<td>FS-ISAC Member</td>
<td>$995 USD</td>
<td>$1,250 USD</td>
</tr>
<tr>
<td>LS-ISAO Member</td>
<td>$995 USD</td>
<td>$1,250 USD</td>
</tr>
<tr>
<td>Government</td>
<td>$1,099 USD</td>
<td>$1,099 USD</td>
</tr>
<tr>
<td>Non-Member (eligible FI only)</td>
<td>$1,099 USD</td>
<td>$1,750 USD</td>
</tr>
<tr>
<td>Monday Dinner Guest Only*</td>
<td>$199 USD</td>
<td>$199 USD</td>
</tr>
<tr>
<td>Guest*</td>
<td>$499 USD</td>
<td>$499 USD</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.

CANCELLATION POLICY

Cancellations received prior to 21 August, 2017 will not be subject to a cancellation fee. Cancellations received on or after 22 August, 2017 will be subject to a $200 cancellation fee. This applies to all members at all tiers as well as non-member, guest, Government and CNOP registration regardless of if a registration fee was paid.

***Any cancellations must be received via email to summit@fsisac.com.***

Registrations are transferable within an organization without penalty.

ONLINE REGISTRATION

fsisac-summit.com/2017-Fall-Attendee-Registration
John Brennan
CIA Director (2013–2017)

*The Cyber Threat: Security Solutions for a Rapidly Changing World*

John O. Brennan was sworn in as director of the Central Intelligence Agency on March 8, 2013. As director, he managed intelligence collection, analysis, covert action, counterintelligence and liaison relationships with foreign intelligence services.

Before becoming director, Brennan served at the White House for four years as assistant to the President for Homeland Security and Counterterrorism. During that time, he advised the President on counterterrorism strategy and helped coordinate the U.S. government’s approach to homeland security, including its policies for responding to terrorism, cyberattacks, natural disasters and pandemics.

Brennan began his service in government at the CIA, where he worked from 1980 to 2005. He spent most of his early career in the agency’s main analytic arm, the Directorate of Intelligence, specializing in the Near East and South Asia before directing counterterrorism analysis in the early 1990s. In 1994 and 1995, he was the agency’s intelligence briefer to President Bill Clinton.

After an assignment as a chief of station in the Middle East, Brennan served from 1999 to 2001 as chief of staff to George Tenet, who was then director of Central Intelligence.

Brennan next worked as deputy executive director of the CIA until 2003, when he began leading a multiagency effort to establish what would become the National Counterterrorism Center. In 2004, he became the center’s interim director. After retiring from the CIA in 2005, Brennan worked in the private sector for three years.

Brennan graduated from Fordham University with a bachelor’s degree in political science. While enrolled at Fordham, he studied abroad at the American University in Cairo. He later attended the University of Texas at Austin, where he earned a master’s degree in government with a concentration in Middle Eastern studies.

Brennan was born in North Bergen, New Jersey. He is married and has three children.
**baltimore, “charm city”**

- Truly a foodie's town, Baltimore has many small, independently-owned restaurants, and few chain restaurants. It’s very easy to find excellent seafood, especially blue crabs, for which Maryland is known.
- Waterfront Promenade is very walkable around the Inner Harbor, which is where the Summit is being held, with lots of nearby attractions.
- **Edgar Allan Poe House** – Poe lived and died (under mysterious circumstances) in Baltimore.
- **Ft. McHenry and the Inner Harbor**
  - The Star Spangled Banner was written by Francis Scott Key as he watched the British bomb Ft. McHenry in the War of 1812. Ft. McHenry protects the Inner Harbor.
  - Britain called Baltimore a “nest of pirates” due to the shipbuilding industry and number of privateers (or privately owned ships authorized by the young American government to harass British ships) that launched from Baltimore. Privateers captured about 5x the number of ships than the U.S. Navy during the three years of the War of 1812. (Source: US Naval Institute)
  - **Tall ships – The Pride of Baltimore** is usually in the Inner Harbor. (Should be in port, but it’s not posted on the schedule yet.)
  - Note: “**Fleet Week**” is the next week starting 8 October! U.S. and Canada Navy and Blue Angel air shows will be happening across the harbor.

**sponsors**

**PLATINUM**

Booz | Allen | Hamilton

**GOLD**

accenture | ANOMALI | AUTHENTIC8 | CENTRIPETAL NETWORKS | Cymmetria | E8 SECURITY

easysolutions | edgile | fireglass | FLASHPOINT | GURUCUL | Predictive Security Analytics

Menlo Security | Microsoft | panaseer | PREVAILENT | pwc | REDOWL

RISKIQ | SailPoint | SecureWorks | SECURITY RISK ADVISORS | SECURONIX | Security Analytics Delivered
Based on member and partner submissions, we have assembled a diverse set of topics and experts including but not limited to topics on Governance, Payments, Resiliency, Technology and Operations, Threat Intel and more.

GENERAL SESSIONS

Addressing Cyberchallenges in Distributed Financial Environments | Modern banking systems have evolved across legislative borders increasing interconnection and complexity. The session will discuss key investment areas within financial environments including data privacy and cross border control; business application segmentation to mitigate advanced threats; and managing operational risk beyond enterprise boundaries.

Automating Internal Threat Reporting and Response - From the Inbox to the SOC | In this talk, PhishMe described how connecting employee phishing reporters to automated response systems dramatically reduces response times and organizational impact through automated collection and propagation of malicious indicators to complementary security detection and prevention technologies. Hear how: - Automation results in 30%+ improvements in IR operational effectiveness - How engagement in reporting reduces overall organizational susceptibility - How real threats are mitigated within minutes rather than hours or days.

MEMBERS ONLY

Adventures in Defending Against a Credential Validation Attack | Credential validation attacks are a constant pain in any organization’s customer login portals. Fending off these attacks can be burdensome and resource intensive, especially when facing adversaries with nearly unlimited sources and computing resources to hide behind. This session details methodologies to identify and block the attacks as well as how to detect canaries being used to block detection.

Adversary Lifecycle Analysis (ALA) Visualization | This session explores a unique approach to cataloging the Adversary Lifecycle Analysis (ALA) a scalable, nation-state agnostic, intelligence driven analytical methodology used to produce a holistic characterization of adversary threats. When presenting a visual representation, analysts can see the pattern of the adversary’s activities and TTPs. This allows for analysts to visualize those changes and potentially pinpoint opportunities to get ahead of the threat and identify potential intelligence gaps to improve the security and reduce risk.

All Quiet on the Digital Front: Security Analytics @ USAA* All Your Defenses Have Failed, Now What?* Application of Analytic Methods in Cyberthreat Risk Malware at Your Service | There is an essential difference between threat intel and attack intel. The former you can spend time analyzing, but the latter you need to block first and analyze later. This is true especially for web-based threats that penetrate your network via compromised digital advertisements (or malvertisements) and content rendering. This session will focus on how web-based malware penetrates your enterprise network, why techniques like ad blocking, whitelisting and blacklisting websites simply don’t work and what to do to strengthen your security posture.

The Reverse Deploy: How Long Does it Take a Single Breach to Affect Requirements Change? | The CISO, internal audit and developers all need to be on the same page when it comes to managing application security. These stakeholders must correctly set the appropriate control points and ensure proper testing for subsequent releases. The challenge is that each stakeholder group has their own process, workflow and mandate. This session will present a lightweight framework that brings together the view points for all of these key application security stakeholders.

Analysis | This session provides an overview of how to access and forecast cyber-risk, utilizing two analytic methods that aid in assessing risk and directing resources - analysis of competing hypothesis (ACH) and the cone of plausibility. The presentation will outline building a threat matrix, assessing risk using ACH, analyzing TTPs and creating a threat forecast.

Building a Crown Jewel Protection Program | In this session, hear how to build a crown jewels protection program. Learn how to identify the location of crown jewels, the steps needed to protect, the detection mechanisms implemented, how to leverage analytics to reduce access and the challenges and opportunities encountered along the way.

Completing the Risk Assessment Cycle: Putting Controls to the Test | The risk assessment (RA) process, identifies the organization’s assets, enumerates the threats against those assets, and provides security controls to protect against those threats. The end of this cycle, and the beginning of the next puts those security controls to the test, validating their ability to protect against threats. Each RA process should begin with an honest assessment of the effectiveness of the existing security controls. This session will offer a variety of tests that may be performed to ensure security controls are working to maximum effectiveness.

*Please check back for more detailed information on this breakout session.
Crisis Communication*

Cyber-Attack Against Payment Systems 2017 | The 2017 FS-ISAC CAPS feature table-top exercises simulating a cyber-attack against electronic corporate trade payments that do not use SWIFT messaging. The exercise's scenario also requires the incident response team to address suspected money laundering associated with the cyber-crime. In this session, hear aggregate anonymous results of surveys completed by the participating incident response teams will be reviewed and join in a discussion about 2018 exercise content.

Cyber-Range Exercises: Lessons Learned for Selecting a Cyber-Range and Having a Successful Exercise in the Range | Cyber-ranges are an exciting new capability to train and test technical teams and new technologies and techniques. Not all cyber-ranges are created equal, however, and the features of a cyber-range will dictate how it benefits your organization. In this session, two different perspectives of cyber-ranges will be presented. The first will discuss types of cyber-ranges, the costs and what to expect from a range-based exercise. The second will discuss the challenges of making range based exercises realistic, keeping a team actively engaged while exercising in a cyber-range and applying lessons learned in the range to real life.

Cybersecurity Advancements for Community Banks*

FS-ISAC Communities Report | Want to know what the FS-ISAC Communities are working on? Or how to get involved? In this session, find out what is happening and how you can get involved.

FS-ISAC Cyber-Range Exercise Project Update | In this session, learn details about a project to evolve the financial sector’s exercise program to include cyber-range/hands-on-keyboard exercises. This new set of exercises will help innovate the sector towards threat-intelligence based scenarios for sector resilience.

Going Beyond Traditional User Behavioral Analytics (UBA): A Real-World Example of Improving Security and Reducing User Friction | Many companies have implemented UBA solutions to provide early detection of security incidents, enabling new, model-driven security controls that have historically been considered prohibitive from a cost or resource standpoint. This presentation will provide insight into implementation, along with real-world results. Examples will include dynamic provisioning, using UBA to influence DLP policies and other, similar situations.

Implementation of Cyber Kill Chain for Cyber-Incident Response | Learn how banks are implementing the Cyber Kill Chain framework for incident response. This session aims to map cyber-attacks to current controls used by the presenters, Cyber Kill Chain phases to current controls and cyber-attacks along with Cyber Kill Chain Phases.

Innovation Challenge*

Internet of Things: Define It Before You Secure It | Within the financial industry, there is no agreed upon definition of the Internet of Things (IoT) as a device category. This lack of definition makes it difficult to have security baselines and fit these devices into current security paradigms. This presentation will propose a definition for IoT and review current threats in the IoT space.

Is the Perimeter Truly Dead? Long Live the Perimeter | In the age of BYOD and Cloud, many have declared the network perimeter dead. In this session, take a first look at the theory behind a defensible perimeter and how it applies in today's technology. Then explore a case study where perimeter theory works and practical challenges still exist.

Maximizing ROI from Penetration Testing | Penetration tests should result in more than just a report that sits on a shelf collecting dust. Establishing a collaborative relationship with your test provider should result in actionable insights that make successful compromise much harder for the practitioner to achieve. This session describes one effective approach to penetration testing.

Mobile Device...Mismanagement? | Virtually everyone has at least one smartphone and add to that the tablets and laptops they carry. To minimize risk, organizations try to tame mobile device management; but rather than minimize access to devices, companies need to develop a better game plan. Data loss prevention (DLP), encryption and mobile device management (MDM) technologies are just a few of the solutions to mitigate risk. During this session, discover how privacy, confidentiality and legal concerns help create a defined game plan to move forward and stay safe.

Moving Your Awareness Program Beyond the Checkbox | This session will detail SANS security awareness maturity model, including elements that can be used in your security awareness program to move up the maturity model, explain the importance of a “security culture” and how this can impact the overall security posture of an organization.

Next Generation Vendor Security Management | It’s safe to say that no company is an island. Your company’s security posture is not strictly determined by your company’s security program alone. Today’s information networks are a patchwork of systems; information shared, exchanged and acquired from multiple sources. In this session, learn about a better approach that leverages core expertise, automation and machine learning to yield both rapid and accurate information necessary to effectively assess and manage vendor security risk.

One Man and an Employee Named SIEM | It’s hard to find good help, especially when you are a one-person IT shop. Sometimes you have to make your own help. This session provides a humorous view of SIEM as an employee and discusses logs, SIEM’s, challenges and successes. If you like logs, alerts and non-repetitive tasks this presentation is for you.

Passive Reconnaissance Techniques for Your Defense | Criminals are searching online for data about your organization and its employees in preparation of their next attack. The enemy is using open-source tools and free services to find email addresses, password leaks, server
names, running services and online profiles to target your organization. This session will demonstrate how you can use these tools and techniques for your defense, trigger alerts when new information about your organization is found online, disrupt the usefulness of the data found and mitigate risk. Learn how a custom-built website comparison tool can be used to monitor homonym domains to target your organization and customers.

Payments 101 | Looking for an introduction to payment types, including credit/debit cards, ACH and wire transfers? Then this session should be at the top of your list! Learn how payments work and insight on attacks currently being leveraged against payment systems.

The Contrarian CISO | When does encryption-at-rest really work? Are organizations going too far in the credential complexity arms-race? When does endpoint control stymie the good guys more than the bad? In this session, challenge, popularly-held assumptions about information security.

Evolving Standards for the Protection of Customer Information in the Retirement Plan Market | There is no consistent industry standard for the protection of customer data in the trillion-dollar retirement plan market. Currently there are a number of competing approaches including the NIST Cybersecurity Framework, BITS, ISO 27001, SOC 2, COBIT and the FFIEC CyberAssessment Tool. This session will share work done by an industry-wide collaboration to establish a uniform risk-based standard for the protection of participant data.

Threat Intel Platforms...Are They Really Worth It? | This session is geared towards helping organizations assemble requirements for threat intelligence platforms (TIPs) including successes, failures and lessons learned from implementation and use.

Toward Harmonization: The Financial Services Sector Cybersecurity Profile | Over the past few years, the financial services sector has been subject to more than 30 different cyber-regulatory proposals or initiatives from more than a dozen government agencies. Many companies now spend up to 40% of their security personnel’s time undertaking compliance related activities rather than critical security activities. This session will step through the proposed sector-specific profile utilizing a unified organizational structure, common language and harmonized baseline for current and future regulatory initiatives.

Tracking Evil on Your Endpoints with Sysmon | This session profiles the journey of a security team that worked for a year to develop a truly cost-effective endpoint detection and response solution that has all the features of much more expensive commercial software. The session will also show how the organization is enriching logs with third-party threat intel and hunting with the data using more advanced analytics.

Using Agile to Secure an Agile SDLC | Participants will learn how to implement the “build security in” principle within the agile/scrum development paradigm. Best practices will be presented featuring agile techniques used to build processes and tools aligned with each sprint evolving the security of the application with each step of the development process.

Why and How Transnational Criminal Enterprises Target the Financial Sector for Cybercrime | Why are transnational criminal enterprises specifically targeting the financial services sector for cybercrime and data breach and is your organization prepared? In this session, attendees will see an eye opening presentation and hear a number of case studies and mitigation strategies with the goal of helping attendees from becoming the next victims.

Winning the Privileged Access War: A Tale About Developers and Privilege | Regulators, auditors and customers have turned up the heat with regards to the proper management of privileged access within financial institutions, especially with developers, the rise of DEVOPS and segregation of duties challenges. In this session, hear experiences with designing prescriptive architecture to address developers with privileged access, and how that architecture was leveraged to reduce regulatory risk and still empower the development process.

CONCURRENT SESSIONS

Automating IR Investigation and Decision Making With Deception | By responding with deception to events in your SIEM and other sources, you can automatically investigate whether they are real attacks. This generates new intelligence from below the threshold and reduces false positives from the analysts’ queue, changing the way we approach our networks in terms of policy. In a greenfield network, any login attempt would be a critical incident. Deception allows us to treat our dirty brownfield networks deterministically instead.

Best Practices for Mitigating Digital Threats Across Web, Mobile and Social Channels | Businesses are embracing new digital channels - web, mobile and social platforms - and cybercriminals are exploiting them. Learn financial industry best practices for automating the detection, investigation and mitigation of modern digital threats across these channels, as well as workflow automation and risk scoring to bridge the collaboration gap between security and legal teams. This presentation will share examples of threats executed across channels, how they can be detected and mitigated utilizing digital threat management frameworks.

Building an Insider Threat Program | Building an insider threat program is much more than feeding logs into a UEBA solution. Effective programs look at user activity, user communications and contextual entity information to create a holistic view of risk that yields actionable insights. In this session, hear best practices based on practical and hands-on experience from multiple organizations, US government agencies and Fortune 100 corporations.
Case Study: Diagnostics Detect, Benchmarking Protects | In this session, learn about smarter technology-risk diagnostics and control plans to detect and provide insights into how benchmarking can protect and inform enterprises in today’s dynamic regulatory environment. The recent updates to the FFIEC Management and Information Security Handbooks, coupled with the recent FTC position enforcing cybersecurity matters necessitated this level of forward thinking to stay ahead of tomorrow’s regulatory and legal requirements.

CISO Case Study: Teaching Old Data New Tricks | Security officers and teams need to communicate with many different business functions to explain risk and justify priorities. Usually this means taking data that is technical and about security and compiling it into an engaging and empowering read for non-technical individuals. This is not without its challenges. Hear how you can give different stakeholders the visibility they need into security-relevant data, so that they understand, support and assist in protecting your business.

Cybersecurity: The Importance of Predictive Technology, Holistic Threat Intelligence and Automated Action | Learn how financial institutions can benefit from big data, machine learning and orchestration to prevent, detect, respond to and predict cybersecurity threats.

Deception-based Threat Detection, Myths and Realities*

Evolving Standards for the Protection of Customer Information in the Retirement Plan Market | There is no consistent industry standard for the protection of customer data in the trillion-dollar retirement plan market. Currently there are a number of competing approaches including the NIST Cybersecurity Framework, BITS, ISO 27001, SOC 2, COBIT and the FFIEC CyberAssessment Tool. This session will share work done by an industry-wide collaboration to establish a uniform risk-based standard for the protection of participant data.

From Threat Assessment to Counter Intelligence: New Web Tools and Techniques | The role of the security team in financial service firms is changing as rapidly as the threat landscape. What used to be static analysis of rogue code delivered to the organization through common communications channels has become a counter-intelligence battle where teams need to understand human and technical threats before they become attacks. Drawing on examples from work with intelligence, defense and treasury organizations, this discussion will focus on the changing role of the analyst and the pressure placed on their normal workflows. Security teams need to create context from raw intelligence, validate source information, monitor threats against the brand and the business. Analysts need to process signals as well as engage in human intelligence functions.

How to Catch a Snowden | Hear lessons learned from Snowden plus other hard-earned wisdom from the latest barrage of high-profile NSA breaches. In this session, learn the steps security leaders can take now to evaluate their readiness to tackle a major breach and address the critical capabilities required to deal with modern cyberthreats.

*Please check back for more detailed information on this breakout session.
To gain full visibility into these threats requires highly-advanced operations security and an intimate familiarity with malicious insider TTPs. This session examines how organizations have utilized Business Risk Intelligence (BRI) derived from the deep and dark web to address and mitigate insider threat scenarios to preserve intellectual property, protect key business assets and uphold brand reputation.

Leveraging Threat Intelligence for Practical Counterintelligence | One of the many benefits of threat intelligence is being able to disrupt adversaries through counterintelligence initiatives. This session will describe cyber-counterintelligence and dive into some practical counterintelligence measures aimed at not only disrupting adversaries but also allowing for the collection of additional intelligence to aid in attribution, situational awareness and overall risk management.

Moving Your Phishing Program Beyond the Checkbox to Change Behavior | This session will provide the audience with two different methods on maturing your phishing simulation training program. Learn about the tools and key elements to use that can help your program move up the maturity model.

Predictive Prevention: Leveraging AI to Get Ahead of the Threat | The word prevention is used alongside words like detect and respond to compare the capabilities of a solution that stops a threat before its impact, versus one that detects a threat post-impact and then attempts to mitigate the damage. But not all prevention is equal. The goal of prevention is to move the threat as far as possible to stop a threat in its tracks, preferably pre-execution and before it can cause damage. What is needed is predictive prevention, a technology that can stop unknown threats without a need for signatures, heuristics, behavior, reputation, cloud look-ups, malware analysis, human interaction and importantly without any delay whatsoever. As we enter the Fourth Industrial Revolution, it is time for financial organizations to take back the rarest resource of all in our battle against the ever-changing threat: time.

Proxy 3.0 - Block and Allow, Meet Isolate. | Proxy solutions are now widely deployed across the financial sector in order to enable employees to be productive online. Current proxy approaches include blocking or allowing access to content and are based on browsing policy, URL categorization, SSL termination and AV. But attacks have evolved quickly and most types of drive-by-downloads, browser exploits, social engineering and phishing attacks developed to bypass proxy filters. In this session, learn about proxy solutions that utilize the concept of isolation, an approach that takes away the inherent risk of browsing without sacrificing employee productivity or enterprise security.

Rethinking Device Identification in Response to Corporate Banking Portal Attacks | Many legacy device identification solutions were originally developed more than a decade ago, with financial service end-users in mind. But as attacks such as targeted malware injections grow in volume and scale, many device identification solutions used by banks have not kept up with the evolution of threats and are growing less accurate over time. This session will propose some innovative techniques for keeping device identification practices current, including a discussion on reducing collision rates and fraud within the sector.

Stopping the Fast Followers: Cybercriminals Leverage Nation State Exploits, and How to Help Disrupt Them | Cybercriminals are increasingly looking for ways to leverage nation-state exploits in their attack campaigns. This session will discuss ways in which the financial services sector can engage to help influence government thinking about use of vulnerabilities, increasing the information flow from governments to the private sector.

The Collision of Data Science and Cybersecurity: Chaos or Utopia? | Machine learning and artificial intelligence are now an important part of the cybersecurity mix. In this session, learn how to advance the practice of behavioral threat hunting and how to best promote those skills within security operations teams.

The Seven Tenets of Successful Identity and Access Management | Corporate networks are disappearing with cloud apps and mobile devices accelerating the ability to make data accessible to users anytime, anywhere. With a focus on privileged user access, this session will cover the seven tenets of a successful identity management strategy regardless of whether an organization deploys on-premises or from the cloud including best practices when designing and integrating their next generation identity access management system.

Tracking Evil on Your Endpoints with Sysmon | This session profiles the journey of a security team that worked for a year to develop a truly cost-effective endpoint detection and response solution that has all the features of much more expensive commercial software. The session will also show how the organization is enriching logs with third-party threat intel and hunting with the data using more advanced analytics.
silver sponsor solutions showcase

Join us for complimentary snacks, 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.

- **Callsign** | Callsign's Intelligence Driven Authentication (IDA)
- **CyberArk** | Protecting Cloud Assets Against Advanced Threats
- **Dome9 Security** | Best Practices to Secure Workloads in Public Cloud Environments
- **Endgame** | Achieving Zero Breach Tolerance: Stop Targeted Attacks Before Damage and Loss
- **IBM** | Uncovering Fraud Faster and More Effectively
- **LookingGlass Cyber Solutions** | Real-Time Threat Killers - Threat Intelligence Gateways and Platforms
- **Lookout** | Managing Mobile Risk in the Enterprise for Security and Compliance
- **ObserevIT** | Best Practices for Building an Insider Threat Program
- **ReversingLabs** | Rebooting Threat Intelligence Sharing and Object Analysis Transparency
- **Skyhigh Networks** | Centralizing Cloud Security With Skyhigh's Cloud Access Security Broker (CASB)
- **Synack** | Quantifying Application Resistance in the Financial Services Industry
- **Unisys** | Biometrics for Identity Management and Security
- **ValiMail** | Regaining Control of Email to Restore Trust and Dramatically Reduce Risk

innovative technology showcase

You will want to make sure to add these showcases to your schedule in Baltimore. 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.

- **Cloud Passage** | Automated Security for the Agile Enterprise
- **Crowdstrike** | Lessons Learned from Recent Investigations of High-Profile Breaches
- **IBM Security** | Where is Cybercrime Really Coming From?
Sunday, 1 October
11:00 a.m.-4:00 p.m. Member Training*
3:00-6:30 p.m. Early Summit Registration
4:30-6:30 p.m. Welcome Reception
7:00-9:00 p.m. Sponsored Member Dinner Events

Monday, 2 October
7:30 a.m.-6:30 p.m. Registration
7:30-8:30 a.m. Breakfast*
8:30-10:00 a.m. Board & Advisors Meeting*
8:30 a.m.-12:15 p.m. Members Only Meetings*
12:15-1:15 p.m. Birds of a Feather Lunch*
1:15-1:45 p.m. Opening Remarks
1:45-2:45 p.m. Keynote
3:00-4:00 p.m. Concurrent Sessions
4:15-5:15 p.m. Silver Solutions Showcase**
5:15-6:30 p.m. Reception
7:00-10:00 p.m. Tailgate Dinner Event - Power Plant Live!

Tuesday, 3 October
7:00 a.m.-7:30 p.m. Registration
7:00-8:00 a.m. Breakfast
8:00-8:15 a.m. Opening Remarks
8:15-9:00 a.m. General Sessions
9:00-10:45 a.m. Concurrent Sessions
10:45-11:15 a.m. Networking Break
11:15 a.m.-12:00 p.m. Concurrent Sessions
12:00-1:15 p.m. Innovative Technology Showcase Lunch
1:15-2:30 p.m. Concurrent Sessions
2:30-3:00 p.m. Networking Break
3:00-4:45 p.m. Concurrent Sessions
5:00-6:00 p.m. Silver Solutions Showcase**
6:00-7:30 p.m. Networking Reception

Wednesday, 4 October
7:00 a.m.-5:00 p.m. Registration
7:00-8:00 a.m. Breakfast
8:00-8:15 a.m. Opening Remarks
8:15-9:15 a.m. General Sessions
9:30-10:15 a.m. Concurrent Sessions
10:15-11:00 a.m. Networking Break
11:00 a.m.-12:00 p.m. Silver Solutions Showcase**
12:00-1:00 p.m. Lunch
1:00-2:30 p.m. Concurrent Sessions
2:30-3:00 p.m. Networking Break & Sponsor Raffle
3:00-3:45 p.m. Concurrent Sessions
4:00-5:00 p.m. Conference Closing Session & Reception
5:30 p.m. Sponsored Member Dinner Events

MISSION STATEMENT
The Financial Services Information Sharing and Analysis Center (FS-ISAC), established in 1999, is a non-profit, member-driven corporation. FS-ISAC’s mission is to help assure the resilience and continuity of the global financial services infrastructure and individual firms against acts that could significantly impact the sector’s ability to provide services critical to the orderly function of the global economy. FS-ISAC shares threat and vulnerability information, conducts coordinated contingency planning exercises, manages rapid response communications for both cyber and physical events, conducts education and training programs and fosters collaborations with and among other key sectors and government agencies. Learn more at fsisac.com

*closed to Sponsor Attendees
**closed to Sponsor Attendees who are not presenting
Agenda is subject to change. For an up-to-date agenda, visit fsisac-summit.com/2017-Fall-Agenda