Date: ***10/1/2017*** ***Time:*** ***11:00 A.M. - 4:00 P.M.*** ***Track:***

Treadstone 71: Intelligence for the C-Suite and Stakeholders Training

Full training description to come. Please check back soon! *Closed to Sponsor attendees.

Speaker Info

First Name	Last Name	Company
Jeff	Bardin	Treadstone 71

Date: ***10/1/2017*** ***Time:*** ***11:00 A.M. - 4:00 P.M.*** ***Track:***

STIX 2.0 Workshop

Full workshop description to come. Please check back soon! This workshop is open to all Summit attendees, including sponsors.

Speaker Info

First Name	Last Name	Company
TBD		Oasis

Date: ***10/2/2017*** ***Time:*** ***10:00 A.M. - 10:45 A.M.*** ***Track:*** ***Technology***

Communities & Working Group Updates

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.

Speaker Info

First Name	Last Name	Company
Rick	Lacafta	FS-ISAC

Date: ***10/2/2017*** ***Time:*** ***10:00 A.M. - 10:45 A.M.*** ***Track:*** ***Threat Intel***

Survival of the Fittest: Evolving Information Sharing Communities

Nature favors individuals that are better at adapting to specific environmental pressures and changes in a way that ensures survival. The cyber equivalent is that organizations who can sense changes to their environment (threats and vulnerabilities) and take action (adapt) in a timely manner are much more likely to maintain operations and limit impact from cyber-attacks. Security Automation and Orchestration (SAO) solutions are being pursued by many organizations as a way to improve the efficiency and effectiveness of their cyber defense activities. A closer look at these solutions shows that their ability to defend is directly related to the organization's ability to sense changes to the environment that have the potential to negatively impact operations. Integrated Cyber Defense acknowledges the critical relationship between the generation and sharing of information with the ability of an organization to dynamically defend itself against attack. This talk will describe how information sharing communities can evolve to promote the sharing of more actionable information, which in turn can be used by local organizations to take more timely and appropriate defensive actions.

Speaker Info

First Name	Last Name	Company
Timothy	Walton	Johns Hopkins Advanced Physics Lab

Date: ***10/2/2017*** ***Time:*** ***10:45 A.M - 11:15 A.M.*** ***Track:*** ***Threat Intel***

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.

Speaker Info

First Name	Last Name	Company
Scott	Augenbaum	Federal Bureau of Investigation

Date: ***10/2/2017*** ***Time:*** ***10:45 A.M. - 11:15 A.M.*** ***Track:*** ***Governance***

Finding Order in Chaos: Using the Cyber Defense Matrix to Map Vendors and Your Security Portfolio

We need consistent ways to define clear categories for the range of products and services that are available in the marketplace to solve our various cybersecurity problems. This highly interactive, roll-up-your-sleeves, facilitated discussion will explore how we can methodically organize the options to remove confusion around the security technologies that we buy and align vendors directly against our gaps and needs.

Speaker Info

First Name	Last Name	Company
Sounil	Yu	Bank of America

Date: ***10/2/2017*** ***Time:*** ***11:30 A.M. - 12:15 P.M.*** ***Track:*** ***Technology***

CISO Panel on Innovation| Innovation Challenge Lunch

A panel of financial industry CISOs and CIOs will challenge the audience to think of innovative ways to meet the latest TTPs in the security and technology areas. Are there ways to increase the cost of an attack to the malicious actors? Should we disrupt the business to protect the business? Can we use existing technology better by understanding why and how adversaries use technology?

Jeff Llungerhofer (CISO, BNY Mellon) will discuss some new ideas in disruptive defensive technology, e.g., seeding credential filers, changing network configurations, honey pot expansions. Jim Routh (CISO, Aetna) will discuss how to work with emerging technology companies to create something that works for your environment.
Responding to emerging cyberthreats require next-generation problem solving and innovation. FS-ISAC is pleased to announce a CISO Innovation Panel and the launch of a MEMBER-ONLY innovation challenge to help succeed in the industry's cyberbattle. Instructions on how to submit your ideas electronically will be provided at the end of the CISO Innovation Panel on Monday morning. All innovative ideas are welcome – an innovative technology or process, new uses of current technology, how to disrupt an attack, how can we force adversaries to use their precious and costly 0-day's, and other ways of increasing the cost or complexity for an attacker. Anything goes! Multiple entries allowed. Starting mid-day Tuesday, Summit attendees will be allowed to vote on their favorite ideas to select the winner. The winner and prize to be announced at the Wednesday General Session.

Speaker Info

First Name	Last Name	Company
Paula	Fetterman	FS-ISAC
Jeff	Llungerhofer	Bank New York Mellon
Jim	Routh	Atena
Carol	Juel	Synchrony Financial
Lynda	Fleury	UNUM

Date: ***10/2/2017*** ***Time:*** ***1:45 P.M. - 2:45 P.M.*** ***Track:***

The Cyber Threat: Security Solutions for a Rapidly Changing World

Session description coming soon!

Speaker Info

First Name	Last Name	Company
John	Brennan	CIA

Date: ***10/2/2017*** ***Time:*** ***2:45 P.M.*** - ***3:15 P.M.*** ***Track:*** ***Governance***

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.

Speaker Info

First Name	Last Name	Company
Dmitry	Kuchynski	Cisco
Anthony	Davis	Cisco

Date: ***10/2/2017*** ***Time:*** ***3:30 P.M.*** - ***4:00 P.M.*** ***Track:*** ***Governance***

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.

Speaker Info

First Name	Last Name	Company
Joshua	Magri	Financial Services Roundtable

Date: ***10/2/2017*** ***Time:*** ***3:30 P.M.*** - ***4:00 P.M.*** ***Track:*** ***Resiliency***

All Your Defenses Have Failed, Now What?

This session details a financial services industry cooperative initiative driving the implementation of an enhanced resiliency model by financial institutions. Learn how banks and brokerages that have adopted the model can offer their customers rapid restoration of access to their assets if the institution’s operations have been severely compromised.

Speaker Info

First Name	Last Name	Company
Steven	Silberstein	Sheltered Harbor LLC

Date: ***10/2/2017*** ***Time:*** ***3:30 P.M.*** ***-*** ***4:00 P.M.*** ***Track:*** ***Payments***

Cyber-Attack Against the 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.

Speaker Info

First Name	Last Name	Company
Charles	Bretz	FS-ISAC

Date: ***10/2/2017*** ***Time:*** ***3:30 P.M.*** ***-*** ***4:00 P.M.*** ***Track:*** ***Threat Intel***

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.

Speaker Info

First Name	Last Name	Company
Colby	DeRodeff	Anomali
Travis	Farral	Anomali

Date: ***10/2/2017*** ***Time:*** ***3:30 P.M.*** ***-*** ***4:00 P.M.*** ***Track:***

Critical Compliance Requirements: Secure File Sharing in Financial Services

Speaker Info

First Name	Last Name	Company
Rick	Lacafta	FS-ISAC

Date: ***10/2/2017*** ***Time:*** ***4:15 P.M.*** ***-*** ***5:15 P.M.*** ***Track:***

Uncovering Fraud Faster and More Effectively

With customers expecting faster and more convenient services, the challenge isn't just intercepting suspicious transactions, but it's also enabling legitimate transactions to proceed without interruption. To more effectively assess the fraud risk, it requires the ability to view account activity in context across channels. IBM offers an approach that helps spot new patterns more quickly, connect the dots to deliver more accurate risk assessments and adaptive intelligence so organizations can adapt faster and apply countermeasures more quickly. Learn more about IBM Trusteer's approach with this demo.

Speaker Info

First Name	Last Name	Company
TBD		IBM Security

Date: ***10/2/2017*** ***Time:*** ***4:15 P.M.*** ***-*** ***5:15 P.M.*** ***Track:***

Protecting Cloud Assets Against Advanced Threats

Accelerating cloud migration requires organizations to implement more effective risk management strategies from the start to better protect cloud assets against advanced threats. This session will explain the security risks posed by advanced threats, steps to secure cloud applications and meet compliance requirements, gain insight into shared responsibility concepts for cloud security and illustrate the importance of mitigating privileged account-related risk.

Speaker Info

First Name	Last Name	Company
Barak	Feldman	CyberArk

Date: ***10/2/2017*** ***Time:*** ***4:15 P.M.*** ***-*** ***5:15 P.M.*** ***Track:***

Centralizing Cloud Security with Skyhigh's Cloud Access Security Broker (CASB)

Gartner advises clients to "deploy CASB for the centralized control of multiple services that would otherwise require individual management". In this session, see how Skyhigh is used to enforce consistent security, compliance and governance policies across cloud services. In this 15-minute lightning demo, see DLP, collaboration control, device access management, threat detection, encryption, cloud discovery, cloud service risk assessment and governance (acceptable use) policy enforcement.

Speaker Info

First Name	Last Name	Company
Doug	Felteau	Skyhigh Networks

Date: ***10/2/2017*** ***Time:*** ***4:15 P.M.*** ***-*** ***5:15 P.M.*** ***Track:***

Real-Time Threat Killers - Threat Intelligence Gateways and Platforms

Threat intelligence has evolved dramatically over the past three years with the volume and speed of threat indicators expanding greatly. Where do CISOs see the greatest impact of automating threat intelligence while also not overburdening their teams? This session will cover real world case studies of applied threat intelligence. Attendees will learn about accurate, low-false positive, real-time threat detection and mitigation while the security infrastructure remains hidden from adversaries.

Speaker Info

First Name	Last Name	Company
Mike	Younkers	LookingGlass Cyber Solutions, Inc.

Date: ***10/2/2017*** ***Time:*** ***4:15 P.M.*** ***-*** ***5:15 P.M.*** ***Track:***

Biometrics for Identity Management and Security

It is a bright picture for the future of biometrics in banking. In this showcase hear how banks can adopt a holistic approach to security and move beyond traditional measures like PINs and passwords.

Speaker Info

First Name	Last Name	Company
Stephen	Migliore	Unisys

Date: ***10/2/2017*** ***Time:*** ***4:15 P.M.*** ***-*** ***5:15 P.M.*** ***Track:***

Rebooting Threat Intelligence Sharing and Object Analysis Transparency

Current threat intel sharing model have not lived up to its potential. Effective sharing starts when you can find what you need rather than what others think that you need. ReversingLabs object analysis technology enables visibility across all embedded objects whether on network, endpoint or storage. In the process ReversingLabs collects information that you and your partners could be interested in while allowing rich YARA retro hunting.

Speaker Info

First Name	Last Name	Company
Mario	Vuksan	ReversingLabs

Date: ***10/2/2017*** ***Time:*** ***8:00 A.M.*** - ***11:00 A.M.*** ***Track:***

The NIST Cybersecurity Framework - CyberSecure My Business Workshop

The CyberSecure My Business workshop, which is designed to teach small and medium-sized businesses about cybersecurity. The workshop is highly interactive and based on adult learning principles, allowing business owners and operators to interact with and learn from their peers, legitimize their current experiences by sharing approaches and apply the learnings to their business. During the 3-hour workshop an NCSA-trained facilitator takes the attendees through the following steps:
1. Understanding assets, "digital crown jewels," they have that others might want to steal.
2. Learning how to protect those assets with limited budgets and time.
3. Detecting when something has gone wrong.
4. Reacting quickly and appropriately to limit the impact and creating a plan of action to remain operational after an incident occurs.
5. Learning what resources are needed to recover after a breach.
*Closed to Sponsor attendees.

Speaker Info

First Name	Last Name	Company
Kristin	Judge	National Cyber Security Alliance

Date: ***10/3/2017*** ***Time:*** ***8:15 A.M.*** - ***8:45 A.M.*** ***Track:*** ***Technology***

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.

Speaker Info

First Name	Last Name	Company
Rohit	Sethi	Security Compass
Jeff	Cohen	TD Ameritrade

Date: ***10/3/2017*** ***Time:*** ***9:00 A.M.*** - ***9:45 A.M.*** ***Track:*** ***Technology***

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.

Speaker Info

First Name	Last Name	Company
Jerry	Perullo	ICE / NYSE

Date: ***10/3/2017*** ***Time:*** ***9:00 A.M.*** - ***9:45 A.M.*** ***Track:*** ***Resiliency***

FSARC Update

Speaker Info

First Name	Last Name	Company
TBD		

Date: ***10/3/2017*** ***Time:*** ***9:00 A.M.*** - ***9:45 A.M.*** ***Track:*** ***Governance***

CISO Case Study: The Why, What, and How of Building an Agile Cybersecurity Analytics Capability

Several technologies, all of which overlap a bit, none of which quite do what we want. This is the reality facing security teams that are trying to make data work smarter for them in measuring, managing and communicating cybersecurity risk. The result? A lack of agility to simplify and automate risk management at the scale and speed that today's business and IT operations require. This CISO case study will share lessons learned on the journey to creating an agile cybersecurity analytics capability that can meet current and future needs of the security team and its stakeholders.

Speaker Info

First Name	Last Name	Company
Nik	Whitfield	Panaseer
Dave	Ritenour	BlackRock

Date: ***10/3/2017*** ***Time:*** ***9:00 A.M.*** - ***9:45 A.M.*** ***Track:*** ***Threat Intel***

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.

Speaker Info

First Name	Last Name	Company
Cristin	Goodwin	Microsoft

Date: ***10/3/2017*** ***Time:*** ***10:00 A.M. - 10:45 A.M.*** ***Track:*** ***Resiliency***

Crisis Communication

Session description coming soon!

Speaker Info

First Name	Last Name	Company
John	Carlson	FS-ISAC

Date: ***10/3/2017*** ***Time:*** ***10:00 A.M. - 10:45 A.M.*** ***Track:*** ***Governance***

Lightening Talks

Lightning talks are designed to be short five-minute discussions on areas that are of greatest interest. FS-ISAC members who have registered for the Summit will receive a survey in August / September to identify which topics are of greatest interest to the Summit attendees. Subject Matter Experts (SMEs) will be sourced from Member organizations, FS-ISAC, and the audience! Topics may include a range of options from nation state attacks, regulatory pressures, the latest threat intel, quantifying cyber threats, and more!

(Note: Survey will be distributed to attendees who were registered by mid-August.)

Speaker Info

First Name	Last Name	Company
Keith	Gerry	Bank of America

Date: ***10/3/2017*** ***Time:*** ***10:00 A.M. - 10:45 A.M.*** ***Track:*** ***Governance***

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.

Speaker Info

First Name	Last Name	Company
David	Deckter	Edgile

Date: ***10/3/2017*** ***Time:*** ***10:00 A.M. - 10:45 A.M.*** ***Track:*** ***Governance***

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.

Speaker Info

First Name	Last Name	Company
Darran	Rolls	SailPoint Technologies

Date: ***10/3/2017*** ***Time:*** ***11:15 A.M. - 12:00 P.M.*** ***Track:*** ***Governance***

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.

Speaker Info

First Name	Last Name	Company
Charles	Bretz	FS-ISAC

Date: ***10/3/2017*** ***Time:*** ***11:15 A.M. - 12:00 P.M.*** ***Track:*** ***Test (App,***

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.

Speaker Info

First Name	Last Name	Company
Greg	Gist	FSISAC
Dr. Shaun	Brady	CMBR

Date: ***10/3/2017*** ***Time:*** ***11:15 A.M - 12:00 P.M.*** ***Track:*** ***Technology***

It's About Sophistication, Not Stupidity. How a Potential Phishing Attack was Spoiled.

The majority of enterprise cyber-attacks begin by compromising a user device via phishing. Once a user device is compromised, the attack can spread across the enterprise. Unfortunately, traditional email security products are not stopping credential theft and malware exploits associated with today's advanced email security attacks. This session will look at how a phishing security auditor was able to successfully execute a sophisticated phishing attack on a community bank that bypassed traditional defenses before being thwarted by isolation technology. How did web documents and powerful scripts fool even the savviest into clicking?

Speaker Info

First Name	Last Name	Company
Kowsik	Guruswamy	Menlo Security
Karl	Kemp	First Community Bank

Date: ***10/3/2017*** ***Time:*** ***11:15 am - 12:00 pm*** ***Track:***

From the Trenches: Top Use Cases for Deception Technology in Financial Institutions

Because cybercriminals will always follow the money, the ability to detect targeted attacks is more than a nice-to-have for banking and securities organizations. This presentation will share insights on how deception approaches can reduce the risk of fraud, mitigate unintentional and malicious insider risk during M&A transitions and help overstretched security teams achieve a more business risk-aligned approach to daily operations.

Speaker Info

First Name	Last Name	Company
TBD		illusive networks

Date: ***10/3/2017*** ***Time:*** ***12:00 P.M. -*** ***Track:***

Automated Security for the Agile Enterprise

Security as an IT deliverable must be as fast, dynamic and agile. As compute models evolve security has to keep up. CloudPassage Halo is automating security with on-demand, high-velocity workload security that works anywhere, at any scale. In this session, see how a 90-second setup with no hardware or virtual appliances to deploy can have you automating security from tens to tens of thousands of workloads, on-demand and wherever you are on your journey to the cloud.

Speaker Info

First Name	Last Name	Company
Rich	Gardner	Cloud Passage

Date: ***10/3/2017*** ***Time:*** ***-*** ***Track:*** ***Innovative***

It's Time to Streamline Your Third-Party Risk Program

According to PwC's 2016 Global State of Information Security report, third-party contractors are the biggest source of security incidents outside of a company's employees. With regulatory scrutiny increasing, outsourcing on the rise and third parties increasingly being leveraged as an attack vector, it's time for third-party risk management to evolve. Fred Kneip, CEO of CyberGRX, will discuss how all organizations can evolve their third-party programs to stay ahead of the threat landscape.

Speaker Info

First Name	Last Name	Company
Fred	Kneip	CyberGRX

Date: ***10/3/2017*** ***Time:*** ***12:00 P.M.*** ***-*** ***Track:***

Lessons Learned from Recent Investigations of High-Profile Breaches

In the past year, CrowdStrike's investigation and remediation of high-profile targeted intrusions have garnered global attention. The stakes have never been higher for private companies, government agencies and nonprofits struggling to protect their networks from highly sophisticated adversaries. Shawn Henry will focus on critical lessons learned in the course of conducting in-depth digital forensics, IR and remediation on behalf of global clients.

Speaker Info

First Name	Last Name	Company
Shawn	Henry	CrowdStrike

Date: ***10/3/2017*** ***Time:*** ***12:00 P.M.*** ***-*** ***Track:***

Where Cybercrime is Really Coming From

Cybercrime is now netting over $450 billion in profits, with over 2 billion records lost or stolen worldwide. Cybersecurity leader Caleb Barlow calls out the inefficiencies in our current strategies to protect our data and the need to respond to cybercrime with the same collective effort we apply to a medical crisis, sharing timely information on who is infected and how the disease is spreading. If we're not sharing, he says, then we're part of the problem.

Speaker Info

First Name	Last Name	Company
Caleb	Barlow	IBM Security

Date: ***10/3/2017*** ***Time:*** ***1:15 P.M.*** ***-*** ***1:45 P.M.*** ***Track:*** ***Resiliency***

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.

Speaker Info

First Name	Last Name	Company
Shailesh	Chirputkar	Bank Leumi

Date: ***10/3/2017*** ***Time:*** ***1:15 P.M.*** ***-*** ***1:45 P.M.*** ***Track:*** ***Technology***

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.

Speaker Info

First Name	Last Name	Company
Mark	Merkow	Charles Schwab and Co., Inc.

Date: ***10/3/2017*** ***Time:*** ***1:15 P.M.*** ***-*** ***1:45 P.M.*** ***Track:*** ***Governance***

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.

Speaker Info

First Name	Last Name	Company
Paul	Valente	Lending Club Corp.

Date: ***10/3/2017*** ***Time:*** ***1:15 P.M.*** ***-*** ***1:45 P.M.*** ***Track:*** ***Governance***

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.

Speaker Info

First Name	Last Name	Company
Chris	Inglis	Securonix

Date: ***10/3/2017*** ***Time:*** ***1:15 P.M.*** ***-*** ***1:45 P.M.*** ***Track:*** ***Technology***

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.

Speaker Info

First Name	Last Name	Company
Josh	Schleicher	Easy Solutions

Date: ***10/3/2017*** ***Time:*** ***2:00 P.M.*** ***-*** ***2:30 P.M.*** ***Track:*** ***Technology***

All Quiet on the Digital Front: Security Analytics @ USAA

Session description coming soon!

Speaker Info

First Name	Last Name	Company
Nelly	Cyrus	USAA

Date: ***10/3/2017*** ***Time:*** ***2:00 P.M.*** ***-*** ***2:30 P.M.*** ***Track:*** ***Governance***

The Future of Tokenized ACH

Bank-to-bank transactions have increased rapidly in 2016 — and the need for strong security has also increased. While tokenization has become standard in the credit card industry, it's seen a slower adoption rate for ACH. This session will highlight how different size institutions approaching tokenization, how to address concerns and the future of ACH tokenization.

Speaker Info

First Name	Last Name	Company
William	Hockey	Plaid

Date: ***10/3/2017*** ***Time:*** ***2:00 P.M.*** ***-*** ***2:30 P.M.*** ***Track:*** ***Governance***

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.

Speaker Info

First Name	Last Name	Company
William	Bailey	Police & Fire FCU

Date: ***10/3/2017*** ***Time:*** ***2:00 P.M.*** ***-*** ***2:30 P.M.*** ***Track:*** ***Threat Intel***

Leveraging Deep & Dark Web Intelligence to Address Insider Threat

Insider threats arise when rogue employees exploit access to their organization's sensitive internal information for personal or political gain. Many organizations focus more on external threats and may not be as focused on potential threats posed by malicious insiders. 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.

Speaker Info

First Name	Last Name	Company
Tom	Hofmann	Flashpoint
Stewart	Draper	Citi Group

Date: ***10/3/2017*** ***Time:*** ***2:00 P.M.*** ***-*** ***2:30 P.M.*** ***Track:*** ***Technology***

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.

Speaker Info

First Name	Last Name	Company
Gadi	Evron	Cymmetria

Date: ***10/3/2017*** ***Time:*** ***3:00 P.M.*** ***-*** ***3:45 P.M.*** ***Track:*** ***Threat Intel***

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.

Speaker Info

First Name	Last Name	Company
Deborah	Janeczek	American Express
Gray	Mauldin	American Express

Date: ***10/3/2017*** ***Time:*** ***3:00 P.M.*** ***-*** ***3:45 P.M.*** ***Track:*** ***Test (App,***

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.

Speaker Info

First Name	Last Name	Company
Adam	Connell	Acadian Asset Management - Old Mutual Asset Management

Date: ***10/3/2017*** ***Time:*** ***3:00 P.M.*** ***-*** ***3:45 P.M.*** ***Track:*** ***Technology***

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.

Speaker Info

First Name	Last Name	Company
Ryan	Keyes	Fifth Third Bancorp

Date: ***10/3/2017*** ***Time:*** ***3:00 P.M.*** ***-*** ***3:45 P.M.*** ***Track:*** ***Governance***

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.

Speaker Info

First Name	Last Name	Company
Tonia	Dudley	Charles Schwab
Brent	Frampton	Vanguard

Date: ***10/3/2017*** ***Time:*** ***3:00 P.M.*** ***-*** ***3:45 P.M.*** ***Track:*** ***Threat Intel***

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.

Speaker Info

First Name	Last Name	Company
Jason	Zann	RiskIQ

Date: ***10/3/2017*** ***Time:*** ***4:00 P.M.*** ***-*** ***4:45 P.M.*** ***Track:*** ***Threat Intel***

Ties Between Government Intelligence Services and Cyber Criminals – Closer Than You Think?

The past year has seen cyberthreat actors arrested, indicted or identified in intelligence reports by US and European governments that many experts believe point to potential ties between government intelligence services and cybercrime actors. In this session learn about the drivers and mechanisms between state and criminal cooperation through a case study that will explore how seemingly ordinary cybercrime can be combined with strategic espionage.

Speaker Info

First Name	Last Name	Company
Nellie	Ohr	Accenture Security
Byron	Collie	Goldman Sachs

Date: ***10/3/2017*** ***Time:*** ***4:00 P.M.*** ***-*** ***4:45 P.M.*** ***Track:*** ***Threat Intel***

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.

Speaker Info

First Name	Last Name	Company
Michael	Young	Bank of America

Date: ***10/3/2017*** ***Time:*** ***4:00 P.M.*** ***-*** ***4:45 P.M.*** ***Track:*** ***Technology***

Supercharge Your SOC with Sysmon

This session reviews a case study for deploying Sysmon to thousands of endpoints, collecting the log data using native Windows features and sending it to SIEM in real-time. Learn about a Sysmon and WEC infrastructure and configuration, as well as recommendations, lessons learnt and how to avoid pitfalls. Hear some of the favorite SIEM rules used to detect evil on endpoints and how to present the data back to analysts for effective investigations. Finally, learn how enrich the logs with third-party threat intel and hunt with the data using more advanced analytics.

Speaker Info

First Name	Last Name	Company
Matt	Giannetto	Susquehanna International Group
Chris	Lee	Susquehanna International Group

Date: ***10/3/2017*** ***Time:*** ***4:00 P.M.*** ***-*** ***4:45 P.M.*** ***Track:*** ***Technology***

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.

Speaker Info

First Name	Last Name	Company
Ravi	Devireddy	E8 Security

Date: ***10/3/2017*** ***Time:*** ***4:00 P.M.*** ***-*** ***4:45 P.M.*** ***Track:*** ***Test (App,***

Improving CyberSOC Performance Though Purple Teams and Freeware

Many financial services organizations are building red, blue and purple team functions in silos. At its best, this approach can create good ad-hoc results. At its worst, this approach misses opportunities to increase coordination, repeatability and measurement. The presenters will discuss a collaborative approach to operationalizing purple teams using freeware for workflow and demonstrating improvement from the earliest simulations.

Speaker Info

First Name	Last Name	Company
Tim	Wainwright	Security Risk Advisors

Date: ***10/3/2017*** ***Time:*** ***5:00 P.M.*** ***-*** ***6:00 P.M.*** ***Track:***

Best Practices for Building an Insider Threat Program

The greatest cyber security threat an organization faces is no longer the malicious outsider hacking from beyond network firewalls. It is the insiders the contractors, vendors, privileged users and business users who already have full access to your company's systems and sensitive data. Addressing this type of threat requires a much different approach than addressing external threats; whether unintentional or malicious, organizations with sensitive customer data need to quickly identify and eliminate insider threat. Attend this session to learn best practices and real life examples for building and maintaining an effective insider threat program.

Speaker Info

First Name	Last Name	Company
Michael	McKee	ObserveIT

Date: ***10/3/2017*** ***Time:*** ***5:00 P.M.*** - ***6:00 P.M.*** ***Track:***

Achieving Zero Breach Tolerance: Stop Targeted Attacks Before Damage and Loss

The banking and financial services industry is constantly targeted by cybercriminals motivated to steal millions of dollars, often causing damage and destruction. Targeted attacks are successful 100% of the time and are not just malware-based. Attacks such as Dridex, Shamoon2 and Odinaff use sophisticated techniques once available only to nation-state actors bypassing existing security programs. In this showcase learn how to pivot existing resources to stop targeted attacks before any damage and loss occurs.

Speaker Info

First Name	Last Name	Company
Mike	Nichols	Endgame

Date: ***10/3/2017*** ***Time:*** ***5:00 P.M.*** - ***6:00 P.M.*** ***Track:***

Callsign's Intelligence Driven Authentication (IDA)

In this showcase see how Callsign's Intelligence Driven Authentication (IDA) solution derives intelligence from raw sensor signals relating to location, device and user-behavior on web and mobile to deliver real-time adaptation of authentication journeys that are appropriate for the level of risk. Hear about the full suite of authenticators which when used together with the intelligence capability can mitigate advanced social engineering and phishing threats.

Speaker Info

First Name	Last Name	Company
Zia	Hayat	Callsign

Date: ***10/3/2017*** ***Time:*** ***5:00 P.M.*** - ***6:00 P.M.*** ***Track:***

Best Practices to Secure Workloads in Public Cloud Environments

Public cloud service providers have beefed up security, yet concerns around securing cloud environments remain high. According to a recent survey of security practitioners, the top barrier to cloud adoption is security. Financial institutions deploying workloads on public clouds at scale are faced with new challenges because traditional tools and controls that worked in the past fail in public cloud environments. This solution spotlight will showcase a new breed of cloud-native security platforms that simplify security operations and enable faster time to compliance.

Speaker Info

First Name	Last Name	Company
Patrick	Pushor	Dome9 Security

Date: ***10/3/2017*** ***Time:*** ***5:00 P.M.*** - ***6:00 P.M.*** ***Track:***

Why Do Less Than Five Percent of US Financial Institutions Achieve Successful Email Authentication

When implemented correctly, email authentication provides a global shield that protects your employees, brand and customers against impersonation attacks and provides complete visibility, control and compliance over cloud services that send email without your approval. Join this session for a discussion around the implementation challenges our industry faces including examples. Also hear about the top business, technical and operational issues and how to solve them.

Speaker Info

First Name	Last Name	Company
Alexander	GarcÃa-Tobar	ValiMail

Date: ***10/3/2017*** ***Time:*** ***5:00 P.M.*** - ***6:00 P.M.*** ***Track:***

Quantifying Application Resistance in the Financial Services Industry

In 2016, the average cost of a data breach in the FS industry exceeded $5.2M. This alarming fact calls into question the exploitability of critical assets. Does your company actually know which assets are susceptible to attack? Traditional pen testing methods have done CISOs a disservice. By measuring security in volume metrics (e.g. # of vulnerabilities found, etc.), pen testers give a limited view of your compliance, rather than a quantified measurement of your systemsâ€™ ability to resist attacks. In order to create an insightful penetration testing report, however, the tester must keep extremely detailed notes and spend days compiling them into an actionable format. We will discuss an approach that allows for the empirical measurement of the pen testing effort. Using this approach, stakeholders can now analyze how hardened their assets really are against the adversary. We attempt to answer the question, â€œhow much effort does an attacker have to exert to compromise my data?

Speaker Info

First Name	Last Name	Company
Mark	Kuhr	Synack

Date: ***10/3/2017*** ***Time:*** ***5:00 pm*** - ***6:00 pm*** ***Track:***

Deception-based Threat Detection, Myths and Realities

In-network threat visibility and detection are considered critical security infrastructure in today's world where advanced threats and insiders consistently demonstrate that they can evade security prevention systems. This Innovative Solutions Showcase session will reveal myths and realities about the effectiveness of deception for detecting advanced threats, operational management efficiency, and what financial services use cases that are driving adoption. You'll also hear about real world deployment experiences, the value financial services customers are realizing, and what pen test Red Teams are saying about this technology. Whether you have an active detection project or are simply curious, this session will provide insight into current financial services market adoption and why deception technology is being chosen as a standard security control.

Speaker Info

First Name	Last Name	Company
Robert	Crisp	Attivo Networks, Inc.

Date: ***10/4/2017*** ***Time:*** ***8:45 A.M. - 9:15 A.M.*** ***Track:*** ***Technology***

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.

Speaker Info

First Name	Last Name	Company
Chris	Olson	The Media Trust

Date: ***10/4/2017*** ***Time:*** ***9:30 A.M. - 10:15 A.M.*** ***Track:*** ***Governance***

Application Of Analytic Methods In Cyberthreat Risk 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.

Speaker Info

First Name	Last Name	Company
Harrison	Kieffer	Goldman Sachs

Date: ***10/4/2017*** ***Time:*** ***9:30 A.M. - 10:15 A.M.*** ***Track:*** ***Governance***

Cybersecurity Advancements for Community Banks

Cybersecurity is more than just an industry buzz-word. With technology continuing to evolve at a rapid pace, keeping technology secure and sound is a challenge for every business. Stay up-to-date on industry-led cybersecurity advancements for your bank. Learn how to enhance your ability to safeguard critical consumer account information in the event that a cyber-attack disables banking operations. In addition, discover why adopting a .BANK web domain will provide a more secure experience for your bank and customers, while protecting against spoofing, phishing and fraud.

Speaker Info

First Name	Last Name	Company
Jeremy	Dalpiaz	Independent Community Bankers of America (ICBA)
Carlos	Recalde	Sheltered Harbor
Andrew	Schiff	fTLD Registry Services

Date: ***10/4/2017*** ***Time:*** ***9:30 A.M.*** - ***10:15 A.M.*** ***Track:*** ***Test (App,***

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.

Speaker Info

First Name	Last Name	Company
John	Falls	American Express
Mike	Brunson	American Express

Date: ***10/4/2017*** ***Time:*** ***9:30 A.M.*** - ***10:15 A.M.*** ***Track:*** ***Governance***

Global Workforce Study: Women in CyberSecurity

The needle has barely moved in terms of the number of women in the cybersecurity workforce despite increased interest in the field, as demonstrated in the 2017 Global Information Security Workforce Study: Women in Cybersecurity. Enterprise and government efforts to attract and retain more women in the global cybersecurity profession have not made a meaningful impact. Although women represent half of the population, the number of female professionals in the field remains stagnant at 11% globally. Women, an underrepresented and underutilized resource to help address a projected workforce gap of 1.8 million cybersecurity professionals by 2022, are a needed element to add to the diversity of thought in our industry as we aim to address changing threats and risks.

This panel will feature accomplished cybersecurity leaders to discuss the results of the Security Workforce Study, examine how women in the security view careers in cybersecurity and identify unique challenges and barriers women face. The panel will highlight insights as well has frame a discussion on what actions organizations should take to address.

Speaker Info

First Name	Last Name	Company
Kelly	Kitch	PwC
Suzanne	Hall	PwC
Meg	Anderson	Principal Financial Group
Julie	Talbot-Hubbard	SunTrust

Date: ***10/4/2017*** ***Time:*** ***9:30 A.M. - 10:15 A.M.*** ***Track:*** ***Technology***

Proxy 3.0 - Block & 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.

Speaker Info

First Name	Last Name	Company
Dan	Amiga	Fireglass

Date: ***10/4/2017*** ***Time:*** ***10:45 A.M. - 11:15 A.M.*** ***Track:*** ***Technology***

Protecting Financial Services Sector Critical Infrastructure: Collaborating with the Department of Homeland Security to Harden Cyber Defense

While the digital age has brought great advancements to the financial services sector, it also has brought great risks. Through a public-private partnership, DHS will develop, test, and evaluate technologies and tools to actively confront advanced adversaries seeking to infiltrate and attack this critical infrastructure. The Next Generation Cyber Infrastructure (NGCI) Apex program addresses the challenges that the financial services sector faces today by providing the tools and technologies to confront cyber-adversaries. The NGCI Apex program collaborates with the financial services sector through the Cyber Apex Review Team (CART) to define and prioritize requirements; conduct planning, testing, and evaluation activities; and carry out the most appropriate methods of technology deployment and transition. Together, DHS and the financial services sector will collaborate to bring solutions for present and future cyber-challenges. This presentation highlights the benefits the financial services sector is accruing by working with DHS to harden cyber-defenses for this critical part of the national economy.

Speaker Info

First Name	Last Name	Company
Greg	Wigton	DHS Science and Technology
Eric	Harder	DHS Science and Technology

Date: ***10/4/2017*** ***Time:*** ***10:45 A.M. - 11:15 A.M.*** ***Track:*** ***Governance***

Cyber Intelligence supporting Fraud Prevention & Detection

In this fast paced panel session, come learn how Cyber Security teams support fraud prevention and detection. Panelists will share lessons learned in their engagement with fraud teams as well as use cases and success stories.

Speaker Info

First Name	Last Name	Company
Kevin	Thomsen	Bank of America

Date: ***10/4/2017*** ***Time:*** ***10:45 A.M. - 11:15 A.M.*** ***Track:*** ***Threat Intel***

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.

Speaker Info

First Name	Last Name	Company
Scott	Petry	Authentic8

Date: ***10/4/2017*** ***Time:*** ***10:45 am - 11:15 am*** ***Track:***

Detecting Breaches Using Deep Visibility into Malware Behaviors

Cybercriminals are extremely creative at slipping past defenses to get a foothold inside a network. A recent survey conducted at Black Hat found that 55% of respondents had suffered a breach. So, the challenge becomes how to detect a network breach before sensitive data is compromised. This presentation describes how breach detection starts with a detailed analysis of specific behaviors that malware is designed to execute that then can be correlated with detected network activity to separate benign activity from seemingly low-risk activity that can be deterministically associated with known malware behavior. The result is high success with detecting network breaches with low false positives.

Speaker Info

First Name	Last Name	Company
Christopher	Kruegel, Ph.D.	Lastline

Date: ***10/4/2017*** ***Time:*** ***8:15 A.M. - 8:45 A.M.*** ***Track:*** ***Technology***

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.

Speaker Info

First Name	Last Name	Company
Aaron	Higbee	PhishMe

Date: ***10/4/2017*** ***Time:*** ***1:00 P.M. - 1:30 P.M.*** ***Track:*** ***Threat Intel***

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 and preempt attacks on your organization and customers.

Speaker Info

First Name	Last Name	Company
David	French	Capital Group

Date: ***10/4/2017*** ***Time:*** ***1:00 P.M. - 1:30 P.M.*** ***Track:*** ***Governance***

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.

Speaker Info

First Name	Last Name	Company
Dennis	Lamm	Fidelity Investments

Date: ***10/4/2017*** ***Time:*** ***1:00 P.M. - 1:30 P.M.*** ***Track:*** ***Threat Intel***

Intelligence Into Action: Security Strategies for Enabling Threat Intelligence

Organizations of all sizes are becoming more secure by implementing the three key components for a threat intelligence program: acquire, aggregate and action. This session will cover current security practices and strategies involving cyberthreat intelligence. Challenges with current security tools will be discussed, best practices identified and how a threat intelligence network defense is providing measurable security benefits in organizations large and small will be explained.

Speaker Info

First Name	Last Name	Company
Jess	Parnell	Centripetal Networks

Date: ***10/4/2017*** ***Time:*** ***1:00 P.M.*** ***-*** ***1:30 P.M.*** ***Track:*** ***Threat Intel***

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.

Speaker Info

First Name	Last Name	Company
Jon	Ramsey	SecureWorks

Date: ***10/4/2017*** ***Time:*** ***1:45 P.M.*** ***-*** ***2:30 P.M.*** ***Track:*** ***Governance***

Key Vendor Risk Areas That Leave You Vulnerable

It's critical to understand your vendor's security controls via periodic risk assessments, but you also need to fill in the gaps in between those assessments. Has the vendor suffered a data breach? Have they had a lawsuit or a fraud investigation? Did they have a phishing attack or an inexplicable credit risk score trend decline? Do you know which of your vendors are preparing to counter today's advanced cyberthreats and which are living in a long-gone era when cybersecurity was limited to a firewall? These points and more are key areas to monitor in vendor risk management what this session is all about.

Speaker Info

First Name	Last Name	Company
Jared	Feinberg	Prevalent

Date: ***10/4/2017*** ***Time:*** ***1:45 P.M.*** ***-*** ***2:30 P.M.*** ***Track:*** ***Technology***

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.

Speaker Info

First Name	Last Name	Company
Dan	Bissmeyer	Huntington National Bank
Guy	Filippelli	RedOwl

Date: ***10/4/2017*** ***Time:*** ***1:45 P.M.*** **-** ***2:30 P.M.*** ***Track:*** ***Governance***

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.

Speaker Info

First Name	Last Name	Company
Christopher	Porter	Fannie Mae
Casey	Andrews	Fannie Mae

Date: ***10/4/2017*** ***Time:*** ***1:45 P.M.*** **-** ***2:30 P.M.*** ***Track:*** ***Technology***

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.

Speaker Info

First Name	Last Name	Company
Jon	Looney	Union Federal Savings And Loan

Date: ***10/4/2017*** ***Time:*** ***3:00 P.M.*** **-** ***3:45 P.M.*** ***Track:*** ***Technology***

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.

Speaker Info

First Name	Last Name	Company
Kurt	Lieber	Aetna

Date: ***10/4/2017*** ***Time:*** ***3:00 P.M.*** - ***3:45 P.M.*** ***Track:*** ***Governance***

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.

Speaker Info

First Name	Last Name	Company
Heather	McCalman	FS-ISAC

Date: ***10/4/2017*** ***Time:*** ***3:00 P.M.*** - ***3:45 P.M.*** ***Track:*** ***Threat Intel***

Threat Intel Platforms...Are They Really Worth It?

This session is geared towards helping organizations assemble requirements for threat intelligence platforms (TIPs). It provides update on Visa's Threat Intelligence Fusion Platform, including successes, failures, and lessons learned over the last 3 years.

Speaker Info

First Name	Last Name	Company
Phil	Desch	Visa

Date: ***10/4/2017*** ***Time:*** ***3:00 P.M.*** - ***3:45 P.M.*** ***Track:*** ***Technology***

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.

Speaker Info

First Name	Last Name	Company
Steve	Horstman	TPG Global

Date: ***10/4/2017*** ***Time:*** ***1:00 P.M.*** ***-*** ***1:30 P.M.*** ***Track:*** ***Technology***

Insider Threats Analytics & Anomalous Behaviors

The threat that looms within. This presentation addresses insider threats, improper employee access and exfiltration of confidential data though the use of behavior analytics including defining problem scenarios, setting objectives, discussing lessons and possible outcomes.

Speaker Info

First Name	Last Name	Company
Ankur	Chadda	Gurucul
Rich	Isenberg	
Nicole	Washburn	Capital One

Date: ***10/4/2017*** ***Time:*** ***1:45 P.M.*** ***-*** ***2:30 P.M.*** ***Track:*** ***Technology***

Ransomware Recovery and Privileged Account Management Improve Resilience

: Malware and insider threat actors often make use of privileged accounts to enable their activities. Recovery from ransomware is complicated by the lack of consistent and protected file and system back-ups. And access rights policies are difficult to enforce using manual processes. The NIST National Cybersecurity Center of Excellence (NCCoE) will discuss its research related to Data Integrity (ransomware recovery), Access Rights Management and Privileged Account Management.

Speaker Info

First Name	Last Name	Company
Harry	Perper	National Cybersecurity Center of Excellence