***Date:* 5/1/2017** ***Time:* 9:45 a.m. - 10:30 a.m.**

## *SWIFT's Customer Security Program - Supporting the Community in Strengthening Security*

Cyber-attacks are growing in number and sophistication and attackers are focusing more deeply inside banks. Recently publicized cases show attackers have started by exploiting security weaknesses within institution's local environments to steal valid operator credentials to their local payment infrastructure. They input seemingly legitimate payment instructions with those valid credentials and hide the evidence of fraud. Combating fraud is a challenge for the whole industry – there are no quick fixes. The threat landscape adapts and evolves by the day, and while customers are responsible for protecting their own environments, SWIFT's Customer Security Program (CSP) has been established to support customers in the fight against cyber-attacks. This session will provide an overview of the program, the successful milestones already achieved and how we continue to jointly work to mitigate the risks of these ever-increasing threats.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Pat | Antonacci | SWIFT |
| Stefano | Ciminelli | SWIFT |

***Date:* 5/1/2017** ***Time:* 10:30 a.m. - 11:15 a.m.**

## *Build Your Cyber A-Team and Strengthen the Cybersecurity Workforce*

Building and maintaining a strong cybersecurity team can be challenging. Employers often struggle to find candidates with the right skills and spend months training them, only to lose them to a competitor. Fortunately, new standards have prompted the creation of programs, tools and guides that can help. In this session, participants will be guided through the tools, templates and information that DHS has developed for organizations as they address cybersecurity workforce planning, recruitment, retention and training issues. Additionally, learn about the National Cybersecurity Workforce Framework and how you can use it to strengthen the cybersecurity workforce!

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Daniel | Stein | United States Department of Homeland Security |

***Date:* 5/1/2017** ***Time:* 11:15 a.m. - 12:00 p.m.**

## *Cloud Migration 2.0: Securing Data in AWS, O365, Slack and Custom Apps*

Currently companies are in the midst of a giant second wave of cloud adoption. In this session explore how the shared responsibility models for AWS/Azure, O365 and Slack differ and the most pressing security risks IT needs to address for each today. Hear results of research into the native security capabilities of each platform and the areas that need supplement native security capabilities to make these services ready for financial services deployments. Finally look at future visions for a data-centric approach to security that transverses all cloud apps.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Rajiv | Gupta | Skyhigh Networks |
| Jason | Witty | U.S. Bank |

***Date:*** ***5/1/2017*** ***Time:*** ***1:15 p.m.*** ***- 2:00 p.m.***

## *FS-ISAC 101*

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| John | Carlson | FS-ISAC |

***Date:*** ***5/1/2017*** ***Time:*** ***2:30 p.m.*** ***- 3:30 p.m.***

## *Cybersecurity in the Age of Espionage*

Recent years have seen a massive increase in cyber theft of private and confidential information from government agencies, business and private individuals. The modern spy is responsible for these attacks. Today's spies are sophisticated, brilliant, devious and technologically advanced, and they are targeting your data. Robert Hanssen was the first of these new cyber spies, charged with selling American secrets to Russia for more than US$1.4 million in cash and diamonds. His ability to exploit computer systems allowed him to protect his identity during a 22 year spy career. Join Eric as he uses real-life spy stories to show how careful diligence, counter espionage techniques and restraint in social media can help identify the numerous spies, hackers, hacktivists and trusted insiders that threaten every stroke of the keyboard.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Eric | O'Neill | Keynote |

***Date:*** ***5/1/2017*** ***Time:*** ***3:45 p.m.*** ***- 4:45 p.m.***

## *The Life of a Trade from InfoSec Perspective*

This presentation will walk through and highlight the internal and external systems used as well as what information is shared to create a trade in the securities industry.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Shannon | Schriver | Susquehanna International Group |
| Josh | Stabiner | Pine River Capital |

***Date:* 5/1/2017 *Time:* 3:45 p.m. - 4:45 p.m.**

## *Disruptive Defense*

It is said that the definition of insanity is repeating the same actions and expecting different results. So, how can we break away from Fiserv "group think" to make it harder for attackers? Is the best defense a good offense? Should we follow the Chinese model of collecting threat intelligence? Join this session to hear from a panel, including industry leaders, who will discuss disruptive defense techniques, some of which may be politically incorrect. Audience participation will be encouraged.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Paula | Fetterman | FS-ISAC |
| Jeff | Lunglhofer | Bank of New York Mellon |
| Tim | Byrd | Wells Fargo |
| Craig | Froelich | Bank of America |
| Gregory | Rattray | JPMorgan Chase |
| Rohan | Amin | JPMorgan Chase |

***Date:* 5/1/2017 *Time:* 3:45 p.m. - 4:45 p.m.**

## *Portraits of the New Cyberdefender: Behind the Looking Glass*

How do security teams change skill-sets and mindsets to defend themselves in the new threat landscape? Created from more than a year of in-depth interviews, this session will present five detailed profiles of the cyberdefense organization, including how teams are structured, staffed, trained and motivated. Learn how teams are weaving in more human and threat intelligence - from understanding the adversary infrastructure, tools and tactics used into the workflows of security operations at a practical level to the benefits and challenges.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Arabella | Hallawell | Arbor Networks, Inc. |

***Date:* 5/1/2017 *Time:* 3:45 p.m. - 4:45 p.m.**

## *Building the Right Team: Successfully Intertwining Cybersecurity and the Legal Team*

You're the security professional who just told the general counsel about a successful cyber-attack on your organization. Who takes the next step, you or legal? Which of you owns the incident response plan? Who is going to contact the CEO? Who is going to brief the Board? What are you required by law to do next? What should you do next? This session will discuss the role the legal department needs to play as part of cyberthreat detection, response planning and execution as well as how to develop a sustainable and cost effective intelligence led solution to cyberdefense.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Colin | McKinty | BAE Systems |
| Tim | Harkness | Freshfields Bruckhaus Deringer US LLP |

***Date:* 5/1/2017** ***Time:* 3:45 p.m. - 4:45 p.m.**

## *Fighting Cybercrime in a Cloud-Based World*

With the move to the cloud, criminal organizations are not changing their targets, but they are evolving their behavior. This session will discuss the evolution of cyber crime and disruptive malware impacting financial institutions and their customers. Learn more about these evolving threats and how using creative legal strategies, with an increased focus to locate the criminal organizations and produce actionable criminal referrals to law enforcement, is helping to facilitate arrests of these criminals. Join this session to learn how Microsoft and FS-ISAC are working to help your organization guard against cyber crime.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Rich | Boscovich | Microsoft |
| Errol | Weiss | Bank of America |

***Date:* 5/1/2017** ***Time:* 5:00 p.m. - 6:00 p.m.**

## *Uncovering the Hidden Keys to Cyber-Insurance*

*With the emergence of new cyber threats, including ransomware and massive DDoS attacks, organizations are increasingly turning to cyber insurance as a method of transferring risk. How can cybersecurity practitioners work collaboratively with internal insurance buyers to negotiate the best rates and ensure the best coverage? Learn a set of best practices for navigating the cyber insurance process, including key lessons learned and issues to watch for.*

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Jacob | Olcott | BitSight Technologies |

***Date:* 5/1/2017** ***Time:* 5:00 p.m. - 6:00 p.m.**

## *Passive Biometrics Beats Fraudsters by Using Their Own Behavior Against Them*

In a time when financial institutions are scrambling to balance risk, security and innovation, while driving excellent customer experience; their bottom line relies on truly knowing who is behind the device. Banks are more vulnerable than ever to automation, ATO, OAO and application fraud. NuData achieves real-time fraud prevention and risk devaluation that truly identifies the good customer – beating fraudsters at their own game. Learn how passive biometrics and behavioral analytics was used to positively verify customer logins at a large commercial bank with near-perfect confidence within only 20 days of implementation as well as immediately helping to reduce false declines, detect good customers and empower the bank to green-path good customers for a great experience.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Ryan | Wilk | NuData Security |

***Date:*** ***5/1/2017*** ***Time:*** ***5:00 p.m. - 6:00 p.m.***

## *Business Risk Intelligence: Shaping the Future of Enterprise Protection*

What makes a security practitioner at a large financial services firm make a career move deeper into providing threat intelligence, more than consuming it? During this session, join Flashpoint to hear from two early adopters of Flashpoint about the challenges faced while navigating the threat intelligence vendor landscape and how these experiences are being used in the present day to provide finished intelligence to Flashpoint customers in the financial services industry.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Chris | Camacho | Flashpoint |
| Glenn | Lemons | **Flashpoint** |

***Date:*** ***5/1/2017*** ***Time:*** ***5:00 p.m. - 6:00 p.m.***

## *How to Identify and Eliminate the Blind Spots for a Drama-Free Security Program, Effective Against the Next 'Next Generation' of Attacks*

A wave of next generation attacks that are 'advanced' and 'unique' has hit. Your exploit prevention and next-gen, math-based malware prevention has been circumvented by ROPless exploits and in-memory attacks. Threat intelligence has become stale, as unique attacks have become the norm. Your SOC is already overwhelmed and anxious of missing never-before-seen attacks and now you are being asked to build a "hunt team" when hunters are scarce or unqualified. In this session learn how to pivot your existing resources to combat the next wave of attacks by focusing on the entire attack life cycle.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Mike | Nichols | Endgame |

***Date:*** ***5/1/2017*** ***Time:*** ***5:00 p.m. - 6:00 p.m.***

## *Using Deception to Hunt Cyber-Attackers*

Used for centuries as a strategy in actual warfare, the concept of deception is becoming a significant weapon in modern network protection schemes. Deception technology doesn't rely on known attack patterns and monitoring. Instead, it employs advanced luring techniques to entice attackers away from valuable company assets and into preset traps, and by doing so, fool them into revealing their presence. This session will outline a deception-based methodology and share the blueprint for a deception layer complete with fake endpoints, servers, services, traffic and data. Learn about new developments that apply active deception and new automation tools that simplify the mass deployment of traps and honey pots as well as new adaptive techniques that allow the deception layer to automatically adjust itself to changing network conditions and best-practices from real-life deployments in leading financial institutes across North America.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Doron | Kolton | TopSpin Security |

***Date:* 5/1/2017** ***Time:* 5:00 p.m. - 6:00 p.m.**

## *Security Essentials When Migrating to the Cloud*

AWS provides enterprises numerous ways to migrate to the cloud, based on your business needs. Because AWS was built with the most data-sensitive, regulated industries in mind, enterprises have access to the most robust networking and security controls to safeguard a protected and seamless migration. In this session, AWS security professionals provide an overview of what security essentials you need to consider when migrating to the cloud. We will also provide a compliance update on what you need to consider in relation to regulatory issues.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Bill | Shinn | Amazon Web Services |

***Date:* 5/1/2017** ***Time:* 5:00 p.m. - 6:00 p.m.**

## *Borderless Behavior Analytics - Top 10 CSO and CISO Insights*

Business has crossed the threshold into a new world of increased productivity and cost savings, yet struggle with how to address security and risk without perimeters. This presentation provides an overview of *Borderless Behavior Analytics - Who's Inside? What're They Doing?*, the new book from Gurucul, which combines the experience and wisdom of nine CSO and CISOs on the security challenges of fragmentation from cloud and mobility driven at customer speed. Additionally, hear the top 10 insights from these thought leaders.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Tom | Clare | Gurucul |

***Date:* 5/1/2017** ***Time:* 5:00 p.m. - 6:00 p.m.**

## *Any Website, Every Email - 100% Secure*

Proxies and mail gateways are failing every day in preventing phishing and malware attacks. Join this session for a live demo on how financial organizations are leveraging Fireglass' True Isolation™ technology to completely eliminate drive-by download, ransomware, spear phishing and other advanced threats and allow users to click with confidence from any device.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Dan | Amiga | Fireglass |

***Date: 5/2/2017*** ***Time: 8:00 a.m. - 8:45 a.m.***

## *Opportunities and Challenges in Engineering Mobile Centric, Omni-Channel Identity for Password Replacement*

Banks and transaction processor application owners are inundating IT and security teams for new requests for identity related projects (such as biometrics), yet the ability for the organization to execute on these requests takes a very long time and costs a lot of money. At the same time, the mobile device is presenting many new opportunities to eliminate passwords and to simplify the identity customer experience across web, mobile, branch and phone channels. This panel will discuss how organizations have made sense of this complex maze, and discuss the next generation of identity architectures being introduced to dramatically reduce internal costs, increasing delivery response times for thousands of use cases and future proofing their environment from vendor lock-in.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Rakesh | Loonkar | Transmit Security, Inc. |
| Matt | Nunn | Citibank |
| David | Fairman | RBC |
| Salim | Hasham | McKinsey |

***Date: 5/2/2017*** ***Time: 8:45 a.m. - 9:15 a.m.***

## *Coming Convergence of Cyberdefense and Information Sharing*

This discussion will focus on the broader convergence of cyberdefense with automated threat sharing and response, and preview new approaches for weaving human collaboration and Machine Readable Threat Intelligence (MRTI)capability together more effectively in assessing potential impacts and defenses across sharing communities in response to cyberthreats.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| George | Johnson | NC4 |
| Sean | Franklin | Franklin Cyber Risk Consulting LLC |
| Wende | Peters | Johns Hopkins University Applied Physics Lab |
| Daniel | Biscoe | NSA- Cyber Task Force |

***Date:*** ***5/2/2017*** ***Time:*** ***9:15 a.m. - 9:45 a.m.***

## *Next-Gen Security Intelligence and Operations Centers - From Training to Cognitive*

Discover how the next generation of SOCs are being built. Moving away from classic IT "moat and castle" approaches towards end-to-end incident handling, cognitive computing and even military grade cybertraining. The session will start with a brief intro into today's approach and examples, including how financial services firms are building next-generation SOCs to handle every aspect from prevention to detection, mitigation, incident response, data sharing and media handling. Learn first-hand from experiences training security teams and doing live SOC simulations. Discover how cognitive computing is evolving into a game changer for security teams fighting fraud and cybercrime. Finally, a discussion around current threats facing the financial industry in areas such as IoT and the latest trends from cybercrime groups using the dark web, including real world examples of how companies are dealing with these security issues.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Etay | Maor | IBM |
| Diana | Kelley | IBM |

***Date:*** ***5/2/2017*** ***Time:*** ***10:15 a.m. - 11:15 a.m.***

## *Demystifying Lateral Movement - A Pragmatic Approach*

After obtaining an initial foothold on an environment, sophisticated attackers need to embark in lateral movement (LM) tasks to be successful in identifying and exfiltrating sensitive information. Being a buzzword, LM is sometimes perceived as a magical thing attackers perform as part of a breach without really understanding it. As defenders, we need to have a clear understating on how LM can be achieved. This presentation will describe how an attacker can perform LMs and what can cyberdefenders do to prevent and detect it.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Mauricio | Velazco | Blackstone |

***Date:*** ***5/2/2017*** ***Time:*** ***10:15 a.m. - 11:15 a.m.***

## *The Dynamic Duo: Threat Intelligence and Security Operations; They Don't Have to be Together to be Great, Do They?*

Representatives from BMO Financial Group, HSBC, and US Bank will present their views and experiences on the collaboration between Threat Intelligence and SOC Functions. What is being done to foster collaboration Innovation and partnership to protect their respective organizations. Going beyond the IOC's and how does the SOC give back. Come and hear from Danell Castro (US Bank), Louise Dandonneau and Vicky Laurens (BMO Financial Group), and Paola Montilla (HSBC) the challenges and surprises separating these two functions bring.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Vicky | Laurens | BMO Financial Group |
| Danell Ann | Castro | U.S Bank |
| Louise | Dandonneau | Scotiabank |

| | | |
|---|---|---|
| Paola | Montilla | HSBC |
| Andrea | Farnsworth | U.S Bank |

***Date: 5/2/2017*** ***Time: 10:15 a.m. - 11:15 a.m.***

## *Security Insiders: Talent Attraction, Retention and Development*

This session will provide tips and tricks about how you can attract, retain and develop talent for information security positions. Learn how to attract interns, entry level and experienced hires including tips for female and diverse hiring, retention and development. Attendees will walk away from the session with tips to take back to their organizations.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Meg | Anderson | Principal |

***Date: 5/2/2017*** ***Time: 10:15 a.m. - 11:15 a.m.***

## *The State of Cyber: How Stealthier Attacks Are Blurring the Lines Between Cybercrime and Statecraft*

Throughout 2016 unprecedented efforts by highly sophisticated adversaries targeting information stolen from sensitive government, corporate and private networks were exposed. These intrusions continue to occur at an alarming rate, reflecting a broad range of motives and targets, and revealing many never-before-seen tactics, techniques and procedures (TTPs) that are advancing the art of data manipulation and attack obfuscation, while raising the bar significantly for organizations seeking to protect themselves from these potentially disruptive and destructive attacks. This session will shed additional light on high-profile incidents and subsequent investigations, while also disclosing invaluable lessons learned and imparting new best practices that can help organizations repel attacks and avoid costly data breaches.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| George | Kurtz | CrowdStrike |

***Date: 5/2/2017*** ***Time: 10:15 a.m. - 11:15 a.m.***

## *Cloud Security - Lessons Learned*

The agility and cost advantages of migrating to public and hybrid cloud environments as well as consuming software-as-a-service are causing significant shifts in how financial institutions (FIs) consume and manage information technology. One of the biggest question marks for FIs is how to support and maintain security and compliance requirements in the cloud. This session will provide lessons learned from real world cloud implementations, present a framework for secure cloud computing and outline best practices for cloud security with a particular focus on how cloud security differs from data center best practices.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Gary | Alterson | Cisco Security |

***Date:*** ***5/2/2017*** ***Time:*** ***11:30 a.m. - 12:30 p.m.***

## *Finding Signal in the Noise: Leveraging Fraud Analytics to Identify Emerging Fraud Schemes*

The diversity of available payment types has led to an evolution of how cybercriminals exploit payment systems for financial gain. These new payment types as well as new technologies developed to combat fraud have led to innovative fraud schemes that require new methodologies to uncover them. Building on sessions from the past three summits, this talk explores how big data analytics can be applied to transactional data to uncover emerging fraud schemes. These analytics allow for the quicker identification of compromised merchants and lead to proactive measures to stop payment card fraud before it occurs. This presentation will provide numerous case studies and detailed methodologies that attendees can leverage in examining their own data.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Christopher | Mascaro | First Data Corporation |

***Date:*** ***5/2/2017*** ***Time:*** ***11:30 a.m. - 12:30 p.m.***

## *The Three T's of Cybersecurity*

Talent, tools and techniques...represent the three T's of cybersecurity. Obviously, the scarcity of talent represents a significant challenge to any enterprise managing a security program. So, which of the T's is the most important? Learn the answer from an industry veteran who will share many examples of unconventional controls that yield favorable business results.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Jim | Routh | Aetna Inc. |

***Date:*** ***5/2/2017*** ***Time:*** ***11:30 a.m. - 12:30 p.m.***

## *Autism and Cybercrime - Profiling Offenders by Behaviors*

More than half of cyber offenders are determined to be on the Autistic Spectrum. The nature of their disorder and the one dimensional, black and white environment of the internet makes technology an attractive draw for people who find the real world difficult to navigate. They find that, due to the nuances of their disorder and their skill set, they can veer into criminal activity without thought for the consequences. A lot of high-profile hacking cases have determined the offender(s) to have an autistic disorder. In this presentation, learn how this conclusion has been arrived at via a study being conducted in the UK with the support of the UK government and law enforcement.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Rebecca | Ledingham | Mastercard |

***Date:* 5/2/2017** ***Time:* 11:30 a.m. - 12:30 p.m.**

## *Deconstructing Elite Credential Theft Services*

Several high-intensity criminal operations dominate the field of credential theft malware, which drives account takeover fraud affecting financials worldwide. Key threats in this area Trickbot, Dridex, Vawtrak, Ramnit, Ursnif and others. This presentation will examine the current characteristics of these organizations and the trajectory of fraud they enable.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| John | Miller | FireEye, Inc. |
| Richard | Hummel | FireEye, Inc. |

***Date:* 5/2/2017** ***Time:* 11:30 a.m. - 12:30 p.m.**

## *Hunting Financial Cyber Criminals*

In order to most effectively identify and eliminate top financial cybercriminals we need to build a broader reaching and more effective intelligence collection net. Very few criminals target a single financial institution, and yet many of us are trying to fight solo and rely solely on the IT security teams to gather threat data. This session will walk through the process of building an all-sources collection plan and how your organization can be a valuable part of a cross-functional and cross-brand investigative team, by bringing together intelligence sources from a variety of sources, including phishing, online forums, social media, suspicious activity reports and FI internal data to build compelling and successful cases.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Gary | Warner | PhishMe |

***Date:* 5/2/2017** ***Time:* 11:30 a.m. - 12:30 p.m.**

## *Subdomain Infringement: When Your Own Domain is Used Against You*

Infringing subdomains are extremely dangerous and destructive to your brand and security posture, enabling phishing, account takeover and fraud from your own registered domain. This session will cover how subdomain infringement works, how prevalent this threat is using five leading financial services companies as real examples, and how FIs can detect and prevent subdomain infringement.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Lou | Manousos | RiskIQ |

***Date:*** ***5/2/2017*** ***Time:*** ***12:30 p.m. - 1:45 p.m.***

## *Change The Game by Taking a Page Out of an Attacker's Playbook*

Millions have been spent on security infrastructure for financial institutions, yet attackers are still penetrating even the most sophisticated prevention defenses. Clearly something has to change. A growing number of financial service companies have turned to new innovations for more efficient continuous threat management (CTM). CTM solutions provide an adaptive defense based on prevention, detection, response and predictability. By using event-based attack information paired with attack path vulnerability assessments, prevention systems are strengthened to block attacks and is forwarded to end-point solutions for forensic artifact threat hunting. Think like a human attacker, leverage the right tools for visibility, detection, and response for continuous threat management to change the game on the attacker. One misstep for them and game over.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Tushar | Kothari | Attivo Networks |

***Date:*** ***5/2/2017*** ***Time:*** ***12:30 p.m. - 1:45 p.m.***

## *How Machine Learning and Artificial Intelligence Will Transform Antivirus*

Invincea is the machine learning next-generation antivirus company dedicated to killing threats without impacting business performance. Invincea proudly protects organizations across the globe by offering a truly new approach to solving today's most challenging security problems through superior security technology; unparalleled performance; utilization of advance techniques to stop the widest range of threats; and open collaboration with industry organizations making business easy and transparent.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Anup | Ghosh | Invincea |

***Date:*** ***5/2/2017*** ***Time:*** ***12:30 p.m. - 1:45 p.m.***

## *Love and Marriage, Fraud Detection and Authentication: You Can't Have One Without the Other*

According to Gartner, absolute identity proofing is dead. After widespread data breaches over the past few years, financial institutions are struggling with legacy authentication solutions, especially in the under-protected call center. The reason? Authentication alone is simply not enough to protect customers and keep the bad guys out. Without a strong fraud detection strategy, fraudsters are enrolling and authenticating using stolen identities, effectively establishing a free reign over customer accounts. In this session learn how fraudsters are bypassing today's call center authentication solutions, including voice biometrics, knowledge based authentication questions (KBA) and caller ID along with innovative new strategies for financial institutions to combine authentication technologies with fraud detection in the call center. Hear about the strengths and weaknesses of current voice biometrics authentication practices, as well as groundbreaking new authentication credentials including analysis of call audio, IVR behavior and DTMF tones.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| **Dr. David** | **Dewey** | Pindrop Security |

***Date:*** ***5/2/2017*** ***Time:*** ***12:30 p.m. - 1:45 p.m.***

## *Proactive Mobile Protection - The Missing Ingredient for Securing iOS and Android*

Real-time proactive protection is the missing element in most mobile security solutions today. Many players have entered the market to detect a variety of threats and attacks. These solutions then integrate with EMM/MDM solutions that enforce enterprise policies, like disabling account access to email. In between detection and remediation, there is a critical gap in time and potentially a roadblock to remediation if the attack is sophisticated. In this session, learn about the protections that must be in place on mobile operating systems, including iOS, to instantly respond to active and predicted threats, to eliminate the opportunity for attackers to view, steal or manipulate sensitive data or gain credentials to attack at a later date.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Adi | Sharabani | Skycure |

***Date:*** ***5/2/2017*** ***Time:*** ***12:30 p.m. - 1:45 p.m.***

## *The Art of the Possible in Threat-Based Assessments*

The current color of “red team” security assessments are “pink” with white-hat hackers doing their best to be “red” but missing the persistent and dynamic approach your adversary is using against your enterprise. For those who desire a truly RED team, imagine having the actual adversarial approach that is gaining access to your enterprise; looking for and finding the best way in. What would this look like? What if you could have a continuously shifting capability against your enterprise, providing the full scope of the approach; run approaches continuously, gaining a real-time view of your enterprise versus once or twice per year; obtain assessments immediately informed by the latest set of threat intelligence or signature-based attack patterns? Join this session to learn about what this possibility can look like.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Bryson | Bort | Grimm |

***Date:*** ***5/2/2017*** ***Time:*** ***12:30 p.m. - 1:45 p.m.***

## *Threat Hunting Beyond the Hype*

Sqrrl is a threat hunting company that enables organizations to target, hunt and disrupt advanced cyber threats. Sqrrl’s threat hunting platform unites link analysis, user and entity behavior analytics (UEBA) and multi-petabyte scalability capabilities into an integrated solution. This unique approach enables security analysts to discover threats faster and reduces the time and resources required to investigate them. Unlike traditional signature- or rule-based detection solutions, Sqrrl’s platform detects the tactics, techniques and procedures (TTPs) of cyber-adversaries using machine learning analytics. Sqrrl leverages network, endpoint, and identity, and threat intelligence datasets and integrates with various security information and event management (SIEM) tools.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Ely | Kahn | Sqrrl |

***Date:*** ***5/2/2017*** ***Time:*** ***1:45 p.m.. - 2:45 p.m.***

## *Cybersecurity Scorecard: Does Your Organization's Security Posture Stand Up?*

The financial industry has a higher cybersecurity maturity than other industries, yet it often fails to prevent modern cyber-attacks, including attacks involving ransomware and polymorphic malware. These failures are spawning more public scrutiny and increased regulatory oversight. To better prevent these attacks, organizations must be able to quickly identify them and close security gaps within their environments. Creating a more mature security posture begins with an honest assessment of where your organization currently stands. This session will detail how organizations can lower their liability against regulatory pressure, reduce security threats to their enterprise, ensure data-security and regulatory accountability and the pressures organizations face when balancing security risks and regulatory mandates. Attendees will leave the session empowered to construct a cybersecurity "scorecard" for their organization, measuring the true regulatory and security postures of their enterprises.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Chris | Strand | Carbon Black |

***Date:*** ***5/2/2017*** ***Time:*** ***1:45 p.m. - 2:45 p.m.***

## *"You're Going to Need a...": Security and Risk Management Lessons from Jaws*

The classic 1975 film, Jaws, presents a unique and fascinating perspective on security threats, risk management and incident handling. The session will examine key scenes from the iconic movie and apply them to real-world security threats that are facing financial institutions. Attendees will leave with a fresh perspective on applying security practices to their organizations. Remember, "it's only an island when you look at it from the water."

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Matthew | Harper | Aflac |

***Date:*** ***5/2/2017*** ***Time:*** ***1:45 p.m. - 2:45 p.m.***

## *Cyber-Exercises: A How-To Guide*

The first session will lay the groundwork for the following two sessions by providing an overview of cyber-exercise fundamentals. This first session will begin by covering the value proposition of exercises and the role of exercises in the preparedness cycle. Following this, industry peers will have a guided tour through the range of exercises available. This will provide an overview of exercise types, a common terminology to reference them and guidance on the most effective way to use them. Building on this foundation, participants will next walk through the planning process and exercise life cycle. Understanding planning timelines and the end-to-end exercise process will provide members with project management background critical to cyber-exercise design. The session will conclude by transitioning from project management details to best practices for building and sustaining an exercise program.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| John | Cosgrove | Citigroup |

***Date:* 5/2/2017** ***Time:* 1:45 p.m. - 2:45 p.m.**

## *Hunting for Security Threats, Lessons Learned from Three Years Building Hunt Teams*

During this session learn about building "hunt" capabilities that search for security breaches including those around SWIFT vulnerabilities. Hunt teams are relative newcomers within the security operations domain. Many companies say they are doing "hunt" but when one digs deeper the capabilities are ad hoc, with no measurable indicators of success nor formal organizational support. That means hunt teams are growing in popularity and use without a "gold standard" for how they work. In this session, lessons learned will be shared transparently so the audience can learn from past experiences. You will leave with a better understanding of what a hunt can be (if run successfully) and a broader view of the ecosystem of breach hunting technology and organizational considerations.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Mary | Karnes Writz | Hewlett Packard Enterprise |

***Date:* 5/2/2017** ***Time:* 1:45 p.m. - 2:45 p.m.**

## *Odinaff: High Stakes Cybercrime*

Since January 2016, campaigns involving malware called Trojan Odinaff have targeted financial organizations worldwide. The attacks are extremely focused on organizations in banking, securities, trading and payroll sectors. The attacks also share links to the Carbanak group, which specializes in high value attacks against financial institutions and has been implicated in a string of attacks against banks and PoS intrusions. This session will discuss the attacker's method of operation and the malware identified during investigation.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Jon | DiMaggio | Symantec Corporation |

***Date:* 5/2/2017** ***Time:* 1:45 p.m. - 2:45 p.m.**

## *Closing the Vault: Defending Your Organization Against Cybercrime-as-a-Service*

Cybercrime-as-a-service (CaaS) is an important trend in deep web forums because it puts cyber criminal tools and services in the hands of a wider range of threat actors—even the nontechnical, such that anyone can become a cyber criminal with minimal investment. Enterprise networks have become targets for evolved versions of CaaS, including Ransomware-as-a Service and even Espionage-as-a-service. This session will provide insight that information security and IT leaders need to know to protect their organizations' critical assets by outlining a typical attack chain and identifying different entry points and evasion techniques utilized by malicious actors. Learn specific steps that information security leaders can implement to guard against evolved threats and the role that innovative technologies, such as machine learning, can play in defending against even hard-to detect threat components such as exploit kits.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Ed | Cabrera | Trend Micro |

***Date:* 5/2/2017** ***Time:* 3:00 p.m. - 4:00 p.m.**

## *Operationalizing the Cyberdefense Matrix*

This is the third part in a series about the Cyberdefense Matrix (CDM) and how it can be used to understand, strengthen and mature one's security program. This session covers how to operationalize the CDM to organize the security team and consistently determine what are the ideal handoffs among business partners. In addition, learn how the CDM can explain and deconflict some of the latest security trends, including microsegmentation, behavior analytics and solutions to destructive attacks.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Sounil | Yu | Bank of America |

***Date:* 5/2/2017** ***Time:* 3:00 p.m. - 4:00 p.m.**

## *Leveraging Threat Intelligence for Small to Mid-Sized FIs 2.0*

Back due to popular demand, this standing room only session is returning for 2017. In this discussion session, hear industry experts share their experiences in utilizing threat intelligence (TI) and automation. Special attention will be given to the unique ways a small or midsize FI can collaborate and participate in TI sharing with the larger community, including building an effective TI program on a shoestring budget, technology implementation (Punch ++, STIX, etc.) and more.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Giles | Ring | Virginia Credit Union |
| Jeff | Jackson | North American Savings Bank |
| Ryan | Moon | Bank of America |
| Justin | Borland | Equifax |

***Date:* 5/2/2017** ***Time:* 3:00 p.m. - 4:00 p.m.**

## *Cyber-Exercise Breakouts*

The second exercise planning breakout session will build off the prior exercise overview presentation. Instruction begins with the most important but most often overlooked aspects of exercise development. Where others cut corners, this session will show how to build it right. The breakout sessions will be divided into two modules: after action reports and evaluation and developing exercise objectives. The first module will begin with the end in mind by addressing effective after action report (AAR) development. Leave this session with a sample AAR and an understanding of exercise evaluation criteria. The second module focuses on the designing an exercise's foundation and exercise objectives. Attendees will understand the importance of exercise objectives and develop two or three specific written objectives.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Mona | Magathan | U.S. Bank |

***Date:* 5/2/2017** ***Time:* 3:00 p.m. - 4:00 p.m.**

## *Ushering in the Era of Big Data Security Analytics*

Security leaders have accepted a realistic but pessimistic outlook – the question is not "if" but "when" their organization will be breached. Those tasked with protecting valuable assets have operated with tools that are incapable of recognizing threats to what they're actually defending: the data! But today, advances in big data analytics, behavior analysis and unsupervised machine learning are enabling real-time detection of threats that were invisible to legacy security tools such as insider threats, fraud, cyber-attacks and abuse of privileged access. This panel presentation will feature insights into new analytical capabilities that predict, prevent, detect and contain threats with unprecedented accuracy.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Nanda | Santhana | Securonix |
| Stewart | Draper | Citi |
| Dave | Helfen | Visa |

***Date:* 5/2/2017** ***Time:* 3:00 p.m. - 4:00 p.m.**

## *An Enhanced Approach to Cybersecurity Risk Assessments: Using Advanced Adversary Simulations to Drive Real World Results*

In this session, learn the benefits of combining a risk assessment with advanced adversary simulation. Hear how leading organizations can evaluate both the maturity and the effectiveness of their information security program to drive an outcome that is a more comprehensive cybersecurity risk assessment and empirical evaluation of their attack resiliency, driving enterprise-wide results.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Chris | Thompson | Accenture |
| Paul | Schutt | Allstate |

***Date:* 5/2/2017** ***Time:* 3:00 p.m. - 4:00 p.m.**

## *Financial Data Protection, Visibility and Control: Security for Regulated Data, Cloud and IoT*

A significant challenge in the financial sector is protecting highly regulated, structured and unstructured data. This data is highly sought after by criminals, yet the ubiquitous sharing of it across platforms and enterprises is essential for financial companies to conduct business. This means unlike most other industries, finance has one of the largest attack surfaces. What is needed is a control that can easily plug into the financial ecosystem and seamlessly provide visibility, control and protection for the most sensitive data. See how top financial companies are approaching some of these challenges within their organizations and understand how a data-centric information protection strategy can enable secure sharing of critical data not only within your own organization but also between consumers, banks, payees, vendors and beyond.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Mike | Bass | Ionic Security |

***Date: 5/2/2017*** ***Time: 4:15 p.m. - 5:15 p.m.***

## *Cyber-Intelligence Meets Information Sharing*

Cyber-intelligence is a crucial component of any cybersecurity program as well as the need to share threat data across verticals. In this session learn the difference between threat data and threat intelligence and more importantly the who/ what/when/where/how of sharing that threat data so your defense can be another companies' offense.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Michael | Slavick | Kaiser Permanente |

***Date: 5/2/2017*** ***Time: 4:15 p.m. - 5:15 p.m.***

## *How to Showcase Your Intelligence Program to Your Board with a Live Attack*

Show your board how tactical intelligence can stop an active attack. This presentation will show you an incredibly impactful way to showcase what an attack looks like, how easy it is to execute and the importance of intelligence in the defense of the network. This session will showcase an incredibly impactful way to highlight the importance of intelligence to an organization by showing how intelligence is used to detect a live attack. A demonstration and all material will be available so you can do this for your executives/board.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Charles | Robertson-Adams | The Capital Group |
| Erin | Nichols | The Capital Group |

***Date: 5/2/2017*** ***Time: 4:15 p.m. - 5:15 p.m.***

## *Live Readiness Exercise*

Applying lessons learned from the prior sessions, the third exercise session will focus on exercise scenario design. This session will provide details on how to safely build a scenario. Placing a scenario within the context of programmatic goals, evaluation criteria and S.M.A.R.T objectives, attendees will take away an understanding of viable and realistic scenarios. More than just an information security staff challenge, members will also learn stakeholders necessary for holistic scenario development. An as interactive session, lively discussion will be encouraged.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| John | Falls | American Express |

***Date:*** ***5/2/2017*** ***Time:*** ***4:15 p.m. - 5:15 p.m.***

## *A Collaborative Approach to Third-Party Risk Management: A Case Study*

In this session, hear about a best practice framework for reducing the potential risk from third-party vendors by developing a collaborative, 'synapse' ecosystem that helps companies both big and small effective manage their vendors. This approach reduces both time to completion and overall cost of evidence collection as well as greatly reducing the risk posed by third parties.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Norman | Menz | Prevalent Inc. |
| Brenda | Ferraro | Aetna Inc. |

***Date:*** ***5/2/2017*** ***Time:*** ***4:15 p.m. - 5:15 p.m.***

## *Why the World's Leading Banks are Inviting Hackers to Help Protect Their Applications and Networks?*

Hackers who help protect billion dollar accounts rather than pilfer them? What has led to this previously unimaginable adoption of crowdsourced security testing by the world's largest financial services institutions? This session will discuss how global banking and financial services institutions are embracing hacker powered, crowdsourced security initiatives to help secure even the most sensitive applications and network environments. In this session, case study examples will be used to show how some of the world's largest banking organizations are currently utilizing crowdsourced teams of trusted ethical hackers to: detect and report holes in critical financial/banking applications and networks to protect highly confidential and valuable information proactively; understand how areas of weakness and subsequent exploitation relates to overall business risk and how vulnerabilities can be prioritized for remediation accordingly; and gain a true understanding of how an adversary views your networks and digital applications.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Christopher | Hudel | Syanck Representative |
| Patrick | Wardle | Synack Representative |

***Date:* 5/2/2017** ***Time:* 4:15 p.m. - 5:15 p.m.**

## *Betrayal-as-a-Service: Trends in Insider Threat*

Insider threat is a trending avenue for malicious actors. Insiders can provide the necessary information and insight into increasingly complex systems, as illustrated by the Bangladesh bank hack in early 2016. Additionally, government agencies are enacting costly regulations, requiring the establishment of corporate insider threat programs. Yet there is no universal definition nor response to insider threat. This session will highlight the shift in insiders due to anonymization and shifting demographics, discuss the coming trends of incremental insider threat and highlight the role that threat intelligence plays in monitoring and identifying indicators of insider threat outside your networks. Also, this session will explore cost effective solutions to implementing continuous monitoring and response to insider breaches, while protecting and respecting the individual privacies of your employees.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| John | Wetzel | Recorded Future |

***Date:* 5/2/2017** ***Time:* 5:30 p.m. - 6:30 p.m.**

## *Say Goodbye to Vulnerability Backlogs: Using RASP to Reclaim Control and Reduce Risk*

Knowing is half the battle when it comes to protecting applications and their sensitive data. Application security testing tools scan your code to reveal long lists of known vulnerabilities, but not all are remediated before the next release. Enterprises resort to using theoretical levels of criticality to prioritize which accumulated vulnerabilities to fix and in what order. Many vulnerabilities often undergo an exception process and make it into production. A real-time, embedded solution like Prevoty's runtime application self-protection (RASP) changes the game completely. Join us to hear case studies on how large financial services organizations eliminated their vulnerability backlogs and began making smarter security operations and remediating decisions.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Kunal | Anand | Prevoty |

***Date:* 5/2/2017** ***Time:* 5:30 p.m. - 6:30 p.m.**

## *Mirai Botnet: A Timeline through the Eyes of the Customer and Provider*

In September, Level 3 began tracking the Mirai botnet, long before it made headlines for crippling East Coast servers and taking its damaging trail westward. Mirai is only one example of the new and sophisticated types of botnets that seek to exploit vulnerabilities – in this case, found in Internet of Things (IoT) devices. In this case study and demonstration walk through the growing sophistication of botnets and how they find new areas of vulnerability to exploit, such as the IoT. Learn the steps global service providers go through in detecting, tracking and mitigating these attacks (before, during and after attacks) through a detailed case study and timeline of the October Mirai botnet incidents.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Chris | Richter | Level 3 Communications |

***Date:* 5/2/2017** ***Time:* 5:30 p.m. - 6:30 p.m.**

## *The Enemy Within: Detecting and Mitigating Insider Threats*

Varonis is a leading provider of software solutions that protect data from insider threats and cyber-attacks. Through an innovative software platform, Varonis allows organizations to analyze, secure, manage and migrate their volumes of unstructured data. Varonis specializes in file and email systems that store valuable spreadsheets, word processing documents, presentations, audio and video files, emails and text. This rapidly growing data often contains an enterprise's financial information, product plans, strategic initiatives, intellectual property, and confidential employee, customer or patient records. IT and business personnel deploy Varonis software for a variety of use cases, including data security, governance and compliance, user behavior analytics, archiving, search and file synchronization and sharing.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Rob | Sobers | Varonis |

***Date:* 5/2/2017** ***Time:* 5:30 p.m. - 6:30 p.m.**

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Tom | Dolan | **ForeScout** |

***Date:* 5/2/2017** ***Time:* 5:30 p.m. - 6:30 p.m.**

## *IoT Security: How to Make the Invisible Visible*

2016 proved to be a phenomenal year for IoT growth and adoption. It was also a year of sobering realities as cybercriminals exploited IoT device vulnerabilities time and again. What are the consequences if an attack on one of these devices shuts down your business? What liability does your business face if your IoT devices are used to attack other organizations? Why are traditional security methods no longer effective in securing enterprise network? During this session, we will address these topics and propose an IoT security strategy for financial organizations. This session will also explain the steps many financial organizations are taking to address these risks.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Robert | McNutt | ForeScout |

***Date:*** ***5/2/2017*** ***Time:*** ***5:30 p.m. - 6:30 p.m.***

## *Building a Blueprint for Financial Industry Security*

A recently completed, comprehensive research study surveyed companies across multiple industries with the goal of discovering how large, complex organizations address application security at scale. The majority of respondents surveyed were multinational organizations who reported annual earnings greater than $1 billion USD. This study has provided novel insights on how the financial industry handles application security at scale. This presentation will reveal aggregated insights, industry trends and best practices that illuminate how financial institutions are addressing application security at scale, so that you may apply and compare these learning's to the state of application security at your own financial institution.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Rohit | Sethi | Security Compass |

***Date:*** ***5/2/2017*** ***Time:*** ***5:30 p.m. - 6:30 p.m.***

## *Cyber-Insurance as Part of a Business Resilience Strategy*

Threats and vulnerabilities abound in the 2017 cyber-environment and every corporation faces the risk of a crippling data breach. Even accidental outages have grown increasingly costly, as more business migrates towards the internet. Risk is unavoidable; even the most rugged cybersecurity footing cannot eliminate the threats faced in today's world. In this presentation, walk through a typical cyber-insurance policy questionnaire and see why an accurate assessment of a company's cyber-risk must include a full scan of the firm's IT environment, including any third-party vendors. This 360-degree view must be buttressed by continuous testing and scanning, keeping up with the rapid changes of a modern data center.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| **Hamish** | **Hawthorn** | UpGuard |

***Date:*** ***5/2/2017*** ***Time:*** ***5:30 p.m. - 6:30 p.m.***

## *Preparing End Users Beyond the Phish*

Despite the increasing number of complex phishing and non-phishing security threats, Wombat's 2016 Beyond the Phish report found significant gaps in end-user awareness and readiness when facing a range of potential threats including safe social media use, mobile device security and data protection. Attend this session to learn how Wombat CyberStrength® Knowledge Assessments and Interactive Training Modules are bridging awareness and training to bring overlooked threat vectors to the forefront and focus on lesser known, but equally as relevant threats. Our interactive training modules focus on more than 20 different topics and offers a flexible, on-demand format that focuses on bite-sized training and includes 508 and WCAG compliant mobile responsive modules.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Joe | Ferrara | Wombat Security Technologies |

***Date:* 5/2/2017** ***Time:* 5:30 p.m. - 6:30 p.m.**

## *Introduction to Kenna: A Risk-Based Approach to Vulnerability Management*

This showcase provides an engaging overview of Kenna, a vulnerability and risk intelligence platform that helps security professionals gain a view of risk across the entire environment as well as prioritize the most critical vulnerabilities. Organizations who struggle with the massive amounts of data generated by vulnerability scanners such as Qualys, Rapid7 or Nessus — as well as those who want to gain a true view of risk, rather than playing the "vulnerability count" game — will be interested in this presentation.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Patrick | Kenny | Kenna Security |

***Date:* 5/3/2017** ***Time:* 8:15 a.m. - 8:45 a.m.**

## *Digital Disruption – But at What Price?*

As financial institutions pursue digital strategies, their operations become part of an evolving and often poorly understood cyber-environment. In this connected ecosystem of entities, people and data, firms are using mobile/social channels to transact. This means organizational perimeters have all but disappeared. We have opened up new avenues of cost-saving, agility and speed-to-market, but at what price? Success will require focus on establishing trust as the blueprint for differentiation in a fast-paced digital world. The confidence with which organizations interact with their stake holders via complex and evolving digital platforms will be enough to make or break a business. In this session, learn how integrating cyber security with digital, companies can deliver value from risk and shift from prevention to ennoblement. By managing traditional and digital risk, companies are well-positioned to defend their businesses, ultimately turning them into digitally trusted partners – both internally with employees, and externally with customers.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| William | Beer | Ernst & Young LLP |
| David | Deane | Ernst & Young LLP |

***Date:* 5/3/2017** ***Time:* 8:45 a.m. - 9:15 a.m.**

## *Fraud Detection and Advanced AI for Cyberthreats*

For many years, financial institutions have been on the bleeding edge of Artificial Intelligence (AI) development as they work to detect and prevent real-time payment fraud around the world. For the past 20 years, FICO has been at the forefront of these developments, working with these institutions to deploy enterprise-grade, machine-learning applications. This session will present how these real-time, self-learning anomaly detection and entity behavior analytics are now being applied to detect cyberthreats and malicious insiders in our digital ecosystem.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Scott | Zoldi | FICO |

***Date:*** ***5/3/2017*** ***Time:*** ***9:30 a.m. - 10:30 a.m.***

## *Will the Real Cyber-Attack Please Stand Up?*

Experts say the next black market is digital certificates. But most organizations don't fully understand how these digital assets are used in cyber-attacks. In this panel discussion, leaders in FS-ISAC member firms will represent both true and false aspects of current advanced cybercrime that misuse certificates, and the audience will test their knowledge using interactive polling. Each panelist will represent a possible attack characteristic—only one will be accurate and the others will highlight common misconceptions. After the audience submits their vote through interactive polling, the "real" cyber-attack will stand up and provide real-world guidance on how to detect, prevent and remediate this type of advanced cyber-attack.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Shelbi | Rombout | Mastercard |
| Shane | Durham | Worldpay |
| Nick | Ritter | Fifth Third Bank |
| Bruce | Phillips | Williston Financial Group |

***Date:*** ***5/3/2017*** ***Time:*** ***9:30 a.m. - 10:30 a.m.***

## *Community Institution Discussion Forum*

An open-floor, panel-led session discussing the successes, trials and pitfalls unique to community institutions. This discussion-driven forum is specifically tailored for community banks and credit unions, with discussion topics sourced from both the panel and the audience. Discussion will include building and maintaining a healthy information security program, threat intelligence for community institutions, risk management and much more.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Wes | Spencer | FNB Bank, Inc. |
| Paul | Moore | Technology Infrastructure FORUM Credit Union |
| Mike | Riggs | Interbank1 |
| Michael | Cole | First Financial Bankshares |

***Date:*** ***5/3/2017*** ***Time:*** ***9:30 a.m. - 10:30 a.m.***

## *Adversary-Centric Threat Hunting and Mitigation*

There are a variety of ways to go threat hunting in an environment. Leveraging threat intelligence to mimic adversaries observed attacking the environment or suspected to have an interest in attacking the environment can be a very effective counter to threats both observed and yet to be seen. This session will focus on a method of threat hunting that involves simulating attacker activity, scouring logs for evidence of that activity and then searching iteratively across the environment for signs of that activity. Additionally, going a step further will discuss how to develop countermeasures and mitigation's against such tools and attacks can carry this approach into a quasi-red team activity.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Colby | DeRodeff | Anomali |
| Travis | Farral | Anomali |

***Date:*** ***5/3/2017*** ***Time:*** ***9:30 a.m. - 10:30 a.m.***

## *Lessons Learned: How to Ramp Up Your Application Security Program*

Most financial services organizations today understand the serious implications of a data breach. At the same time, most may not be funneling enough money or resources toward application security – an initiative that could greatly reduce the risk of a data breach. This disconnect can stem in part from simply not knowing where to start. In this session, learn about getting started with application security, getting teams on board with application security, integrating security into development processes, measuring AppSec success and managing and maturing an application security program.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Gary | Nichols | Charles Schwab |
| Andrew | Schofield | Charles Schwab |

***Date:* 5/3/2017** ***Time:* 10:45 a.m. - 11:45 a.m.**

## *Minimizing Fraud and Risk at New Account Onboarding through Advanced Identity and Authentication Solutions*

In 2017 and beyond, Financial Institutions (FIs) will face challenges to identify and authenticate new customers, especially as digital-natives demand access in convenient, faceless environments. As the industry shifts, decision making must rely on more advanced solutions to help offset the risk in digital channels, such as predictive analytics, machine learning, passive and active biometrics. With the convergence of fraud and cyber security, the banks are looking at enterprise solutions for authentication.
During this demo, attendees will see how Early Warning's *Authentify*® Platform Solution Suite utilizes traditional login with two factor authentication through one time passcodes and authentifiers. In addition, you will see passwordless logins and authentication using a mobile app. Finally, see how Fortified OTP Link can help provide a secure solution for your organization. To learn more, visit www.earlywarning.com.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Glen | Sgambati | Early Warning |

***Date:* 5/3/2017** ***Time:* 10:45 a.m. - 11:45 a.m.**

## *How The Cloud Allows Ransomware to Hide in Plain Sight*

Cloud services are alive and well in financial services organizations and with them come threats and malware. Malware takes advantage of the cloud's best features to propagate itself to more users and across organizational lines. The Netskope Threat Labs has identified the top five types of malware most commonly found in banks, insurance companies and investment firms. Participants will learn the top five threats found in financial organizations' cloud services, and how they got there; which types carry ransomware; how malware propagates in the cloud and creates a dangerous "fan-out" effect; and what financial organizations can do to protect themselves today.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Bob | Gilbert | Netskope |

***Date:* 5/3/2017** ***Time:* 10:45 a.m. - 11:45 a.m.**

## *Defuse the Data Bomb*

Businesses are challenged with protecting a growing amount of data which is sensitive and a ticking time bomb. In most industries, if you have sensitive information you must protect it. At the same time, protection requirements are continually evolving and becoming increasingly more complex. Financial institutions are faced with a myriad of regulatory, compliance and contractual requirements to protect critical data and if your organization's sensitive information crosses country borders, additional sets of requirements apply. This session will help you prevent the next data breach by defusing this ticking time bomb.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Buck | Bell | Optiv |

***Date:*** ***5/3/2017*** ***Time:*** ***10:45 a.m. - 11:45 a.m.***

## *DevOps and Software Risk for Highly Regulated Industries*

This session will cover how security leaders in highly regulated industries are trying to adapt their software security programs to the realities of DevOps. By no means is software security solved, yet there is an imperative from businesses to implement concepts. Security leaders in regulated industry are trying to adapt, balancing security needs with the inevitable questions that will come from financial examiners. Learn about DevOps, agile development and continuous integration/continuous deployment (CI/CD) and how security leaders in regulated industries are balancing DevOps, security and audit risk while addressing the need to go faster and be even more competitive.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| John | Dickson | Denim Group |

***Date:*** ***5/3/2017*** ***Time:*** ***10:45 a.m. - 11:45 a.m.***

## *Identify and Protect Sensitive Data Across the Enterprise*

TITUS classification solutions enable financial organizations to identify, classify and secure their unstructured data. A foundation of classified unstructured data supports successful cybersecurity initiatives including data governance programs, security policy optimization and enhanced data protection. Critical for large enterprises today, TITUS solutions help foster a culture of security be engaging employees to classify, and thereby protect, information in emails, documents and other file types – on premise, on mobile devices and in the Cloud.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Tim | Upton | TITUS |

***Date:*** ***5/3/2017*** ***Time:*** ***10:45 a.m. - 11:45 a.m.***

## *Industry Best Scan Engine Effectively Powers IT Security Automation Platforms*

Organizations around the globe are striving to create a healthy security ecosystem and integration with multiple solutions in an effort to take a holistic approach to security. However, if organizations are integrating with vulnerability management solutions that are not producing accurate scanning results, critical decisions could be based on faulty data. Cybersecurity programs encompass a significant amount of data to filter and sort through to identify the critical information. Introduction of bad data could cripple your cybersecurity program procedures and processes. Digital Defense will demonstrate how organizations can ensure they get the most accurate vulnerability scan data to help alleviate security data overload and bridge the gap between IT and security operations to efficiently operationalize their cybersecurity program.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Gordon | MacKay | Digital Defense, Inc. |

***Date:* 5/3/2017** ***Time:* 10:45 a.m. - 11:45 a.m.**

## *You Have Threat Intelligence in Your Arsenal, So What?*

The life of a security professional is a constant battle: defending against cybercriminals and increasingly sophisticated malware delivery methods, suffering from a death of human resources and overload of security solutions, all while walking through a labyrinth of ever evolving regulations. Securing budget to fund resources and build an effective strategy entails another skirmish, but this time with executive management. And, every dollar counts. How do InfoSec professionals know if threat intelligence is delivering the expected protection? Learn how to create a winning threat intelligence strategy through this presentation, which will walk the audience through a series of questions (and answers) about the enterprise's treat intelligence strategy.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Chris | Olson | The Media Trust |

***Date:* 5/3/2017** ***Time:* 10:45 a.m. - 11:45 a.m.**

## *Isolation as the New Security Standard for Bank Security*

This discussion will illuminate how isolation security technology can protect banks from the leading malware threat vectors that account for 90% of security risk for banks and financial institutions – web and email. Unlike traditional security approaches, isolation eliminates 100 percent of malware, ransomware and phishing threats because it does not use the traditional “good v. bad” detection and prevention methods. With an isolation approach, all content is made harmless and only malware-free rendering information is sent to the user devices, where no software is required and users do not have to update. This protects financial institutions from cyber-attacks by isolating and rendering the most common document types.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Kowsik | Guruswamy | Menlo Security |

***Date:* 5/3/2017** ***Time:* 1:30 p.m. - 2:00 p.m.**

## *Financial Services Cyber-Regulations and RegTech: Emerging Trends, Opportunities and Risks*

Increasing regulatory and threat environments are driving organizations to demand more from their cybersolutions. While new rules and regulations such as those from the New York State Department of Financial Services, Federal Financial Institutions Examination Council and the EU’s General Data Protection Regulation are requiring more prescriptive frameworks than existing regulations, increasing cybersolution complexity. This presentation will explore topics such as what impacts the new regulations have on existing operations; how CISOs and CROs should work together to stay focused on the organization’s risk and threat tract while remaining compliant; and what is adhering to these new regulations going to cost.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| **Dave** | **Wilson** | Deloitte |
| Marcia | Peters | U.S. Bank |
| David | Cowart | Chubb |
| Sydney | Klein | Capital One |

***Date:* 5/3/2017** ***Time:* 1:30 p.m. - 2:00 p.m.**

## *Use Case: How One Global Bank Utilized Security Analytics to Mitigate Fraud*

Fraud costs financial services companies hundreds of millions of dollars every year. Existing detection products are unable to surface fraud on a broad spectrum. Security analytics offers a new approach to fraud detection for both employees and online. This presentation will detail the implementation of a fraud detection project featuring the use of advanced security/behavioral analytics. Learn how a security analytics product can be utilized successfully, best practices and lesson learned from the project deployment and ongoing operations.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Stephan | Jou | **Interset Software** |

***Date:* 5/3/2017** ***Time:* 1:30 p.m. - 2:00 p.m.**

## *Financial Services Social Engineering and CEO Fraud: the $2.3 Billion Mistake*

Social engineering methods and the “evil genius” of CEO fraud are costing businesses billions of dollars with little chance of recovery. Ransomware is one of the top three most dangerous security threats and continues to proliferate despite the best efforts of endpoint security and gateway solutions to block them. How do you manage the ongoing problem of users falling for social engineering attacks and what are the most effective methods for securing your organization to combat cybercrime? This presentation will cover how financial institutions can stay ahead of social engineering traps and lower risk.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Stu | Sjouwerman | KnowBe4 |

***Date:* 5/3/2017** ***Time:* 1:30 p.m. - 2:30 p.m.**

## *Case Study on Service Catalog and Three-Lines of Defense*

The recent updates to the FFIEC Management and Information Security Handbooks necessitate a highly organized level of alignment. Not to mention today’s cyberthreats require this level of coordination and collaboration. This presentation details a case study on operationalizing information risk management policies across three lines of defense using a service catalog. Learn how the service catalog approach allows organizations to clearly define roles and responsibilities between front line risk takers, second line risk oversight and third line audit providing accountability and enabling a glide path for a maturity roadmap to incrementally improve the service capabilities over time.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| David | Deckter | Edgile |
| Geoff | Hauge | Edgile |

***Date:* 5/3/2017** ***Time:* 2:10 p.m. - 2:40 p.m.**

## *Ducking Threats Globally - Threat Management for the Global Organization*

Threat management has evolved becoming a critical component of a mature security program. For many businesses, this means that threat intelligence processes and systems must expand beyond domestic headquarters. This session will discuss successes and lessons learned in taking a cutting-edge threat intelligence platform used in one country and expanding its accessibility, user base, architecture and processes to support around-the-clock operation, analysis and control deployment in multiple geographic office locations. Topics discussed will include architecture considerations, legal and compliance hurdles, cultural nuances, process design and tangible results.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Ben | Murphy | Aflac |

***Date:* 5/3/2017** ***Time:* 2:50 p.m. - 3:20 p.m.**

## *Non-Conventional Data Gathering Using Huginn and Elasticsearch*

Today's InfoSec world is a fast-paced society in which vast data is available at people's fingertips. Searching, organizing and deleting relevant information from this data is the key to succeeding in accurately stopping threats in a timely manner. This session will discuss and showcase the dual usage of Huginn and Elasticsearch to implement the automatic monitoring of several sources of useful unstructured information at a minimal cost to the organization.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Ryan | Keyes | Fifth Third Bank |

***Date:* 5/3/2017** ***Time:* 2:10 p.m. - 2:40 p.m.**

## *Steganography-Stealing Data in Plain Sight*

Stealing data is easier than you think and could happen right in front of you. Concealing data within multimedia, operating systems and network traffic provides covert transfer of valuable data. The art of sending covert messages has been around for thousands of years and modern technology has facilitated the ability to hide messages (and data) in common media to avoid detection. As technology changes, the methods of stealthy communications seems to get easier to conduct but harder to detect. This presentation will explore various approaches to hiding data and covert communications. It will explore the tools and techniques used to hide this data in common transport carriers as well as provide a broad understanding of how these methods work. Armed with this information, participants will be better able to identify where they may be at risk for data exfiltration via steganography.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| David | Plude | Genworth Financial |

***Date:* 5/3/2017** ***Time:* 2:10 p.m. - 2:40 p.m.**

## *Cybersecurity: Threat Landscape and Internal Audit*

This session will focus on how an internal audit of your organization can provide details on coverage of cybersecurity. Topics that will be discussed include: the cyberthreat landscape – actors and methods, current cyberthreat trends, knowing the enemy, insider threat, "attacker already has access", cyber-attacks, internal audit best practices, information security auditor engagement model, "defense in depth" audit coverage and audit coverage mapped to key risks.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Patricia | Voight | Citi |

***Date:* 5/3/2017** ***Time:* 2:50 p.m. - 3:20 p,m.**

## *Sector-Level Crisis Communication Playbooks*

The Communication Playbooks are of great interest to CISO, CROs and operations leaders because they solve a problem of helping companies define the external messaging on a breach or significant disruption event. This session will discuss new education and utilizations of the Communication Playbooks and the All-Hazards Playbook crisis response process.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Susan | Rogers | FS-ISAC |

***Date:* 5/3/2017** ***Time:* 2:50 p.m. - 3:20 p.m.**

## *Sector-Level Crisis Communication Playbooks*

The Communication Playbooks are of great interest to CISO, CROs and operations leaders because they solve a problem of helping companies define the external messaging on a breach or significant disruption event. This session will discuss new education and utilizations of the Communication Playbooks and the All-Hazards Playbook crisis response process

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| John | Di Nuzzo | Synchrony Financial |

***Date:*** ***5/3/2017*** ***Time:*** ***2:50 p.m. - 3:20 p.m.***

## *Where Privacy and Security Intersect*

Information security and information privacy are not the same. Regulations are looking towards a risk assessment, which looks at the threats, vulnerabilities and the likelihood that those events will represent a risk to the organization based on their likelihood and impact. One of the largest risks today is that of unauthorized information disclosure. There are an increasing number of privacy concerns that security managers need to start becoming familiar with. While they don't need to become attorneys, they need to realize the requests that various legal entities will request. Keeping a secure system is a great step, but if privacy isn't part of the decision process, the secure system stays secure only for so long. Understanding the privacy requirements helps the security manager prioritize their efforts. When security ultimately fails, whether due to a technical or process-based reason, the privacy protections help limit the exposure of the incident.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| William | Bailey | Police & Fire FCU |

***Date:*** ***5/3/2017*** ***Time:*** ***2:50 p.m. - 3:20 p.m.***

## *Myths of Cybersecurity*

This presentation will shed light on some of the various myths amongst information technology professionals and others about cybersecurity controls and how effective they are in reality. Some misconceptions are dangerous to organizations in that they may believe a control or set of controls make them safe from malware and other forms of maliciousness. This presentation will clarify and correct some of these common misconceptions. Participants should leave the session with a better understanding of what certain common controls do for them and what they don't do.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Greg | Jones | Progess Bank |

***Date:*** ***5/3/2017*** ***Time:*** ***3:30 p.m. - 4:00 p.m.***

## *DMARC Quick Start Guide*

This session is a practical discussion on the implementation of DMARC for financial institutions. Learn actionable items to assist in implementation and adoption as well as best practices for a smooth transition.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Don | Cardinal | Bank of America |

***Date: 5/3/2017*** ***Time: 3:30 p.m. - 4:00 p.m.***

## *Board Reporting is Not Boring*

Many boards discuss cybersecurity with management when cyber attacks are widely reported or when the financial institution experiences an attack. However, routinely discussing cybersecurity issues in board and senior management meetings will help the financial institution set the tone from the top and build a security culture. In this panel presentation, learn what some community institutions are doing to inform and educate their boards.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Heather | McCalman | FS-ISAC |
| Thomas | Henricks | Clearview FCU |

***Date: 5/3/2017*** ***Time: 4:10 p.m. - 4:40 p.m.***

## *From Consumer to Producer: Taking Your Community Institution to the Next Level*

Are you interested in doing more than consuming intelligence, and learning how to join the fight against malware and other threats? It is vital to the health of a sharing community that everyone do what they can to contribute, but many of us are not sure how or where to start. Well, with very little time and commitment we can generate valuable data as well as sharpen our senses in defending our own institutions. This session will share some simple ways to take your institution from a threat intelligence consumer to a threat intelligence producer by covering topics like data visualization (email and web), malware and endpoint analysis, network forensics and honeypots.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| John | Lockie | Caltech Employees Federal Credit Union |

***Date: 5/3/2017*** ***Time: 4:10 p.m. - 4:40 p.m.***

## *Building a Risk Assessment Process for Small Institutions*

Safeguarding an institutions critical information assets and systems has never been more important in the age of evolving cyber threats. Enterprise risk management (ERM) is a fundamental approach for the management of an organization. IT enterprise security risk assessments are performed to allow organizations to assess, identify and modify their overall security posture and to enable security, operations, organizational management and other personnel to collaborate and view the entire organization from an attacker's perspective. In this presentation, learn how small institutions have built an effective risk assessment program and increased the overall security culture in their organizations.

***Speaker Info***

| First Name | Last Name | Company |
|---|---|---|
| Jeffrey | Korte | FS-ISAC |
| Joseph | Arahill | Customers Bank |
| Monica | Rowe | Mazuma Credit Union |
| Lynn | English | Lafayette FCN |

***Date:*** ***5/3/2017*** ***Time:*** ***4:10 p.m. - 4:40 p.m.***

## *Avoiding APT Misattribution with Indicators of Deception*

Advanced persistent threat (APT) cyber-attacks—orchestrated by sophisticated criminal groups or by state-sponsored hackers—always employ a level of deception by misdirecting pursuers into misattribution. Cybersecurity researchers are already burdened by their competitive commercial landscape in post-incident reporting and today's media outlets often prioritize speed and sensationalism that may cause cyber-attacks to be attributed too quickly. To the benefit of APTs this pressure can lead to misattribution caused by poor due diligence enabled by analytical errors and shortsightedness. Consequently, cybersecurity researchers need a logical approach to discover indicators of deception (IoD) and avoid APT misattribution. Because APTs easily and effectively employ deception to evade responsibility and retribution, the trend will likely continue due to ever competing financial and political-military interests. This session aims to enhance cybersecurity researchers' ability to identify IoD and confirm the misdirection – even under rapid publication deadlines.

***Speaker Info***


| First Name | Last Name | Company |
|---|---|---|
| Artur | Taryan | First Data Corporation |