

Date: 1/10/2018

Time: 10:30 – 11:00

Track: Threat Intelligence and Law

A Standard Model for Threat Intelligence Practices: Agile Threat Intelligence

Threat Intelligence as a practice has been evolving over the past few years and has finally seen common patterns and best practices emerging. This session will outline how this thinking emerged and the best practices in implementing a threat intelligence practice - people, process and technology. Gain a clear understanding of how to plan and take steps towards a common model based on best practices and understanding what drives success and failure in threat intelligence.

Speaker Info

First Name	Last Name	Company
Joep	Gommers	Eclectic IQ

Date: 1/10/2018

Time: 11:15 – 12:00

Track: Governance, Risk, and Compliance

Why Visualize

Our society has never been more data rich – 90% of the world’s data has been generated in the past two years - including the exponential growth in cybersecurity data used to safeguard our organizations. How do you increase understanding of this data and provide the knowledge back in an easily understood and readily accessible way? The answer lies in data visualization. Join this session to explore the benefits of visualization and how it can be used to identify actionable data faster, enable better prioritization and best practice examples.

Speaker Info

First Name	Last Name	Company
Alex	Hale	FMR

Date: 1/10/2018

Time: 11:15 – 12:00

Track: Technology and Operations

Threat Intelligence Driven Incident Response

Join this session to learn how the Nordic Financial CERT (NFCERT) works with threat intelligence and tracks threats to prepare members for an eventual attack. Explore technical tracking of IOCs and the threat actor, preparing the detection and testing that detection works and working with law enforcement to ensure they understand the scenario when the victims start to file the complaints.

Speaker Info

First Name	Last Name	Company
Per Morten	Sandstad	Nordic Financial CERT

Date: 1/10/2018

Time: 11:15 – 12:00

Track: Threat Intelligence and Law

Cybercriminal Ecosystem DNA: Finding Strength and Resilience in Diversity

Explore the evolution of the dark-web from inefficient peer-to-peer “enterprises” in its early days, to the highly specialized, economy of today. This session will outline the essential support-services that help miscreants target individuals and organizations in Western Europe, North America and Oceania. Additionally, this session will discuss the operations of the biggest underground marketplaces that specialize in the resale of compromised payment information.

Speaker Info

First Name	Last Name	Company
Andrea	Barysevich	Recorded Future

Date: 1/10/2018

Time: 11:15 – 12:00

Track:

ETIC and ESC Update

In this session join ETIC and ESC representatives for a look at what their respective groups have been working on and a look at updates and highlights of initiatives.

Speaker Info

First Name	Last Name	Company
Tania	Brown	Deutsche Bank

Date: 1/10/2018

Time: 12:15 – 12:45

Track: Threat Intelligence and Law

A Strategic Response to the Booming Trade in Cyber Criminality

The nature of cyberthreats is escalating. This session will explore some of the challenges facing the financial services industry as well as the potential opportunities that lie ahead. Learn about what the melding of physical, social and digital attacks and the collaboration of actor groups means for organisations mounting their best strategic response, as well as the importance of public- and private-sector community collaborations to battle those within criminal enterprises. Finally, learn how better data integration, data science and intelligence-led solutions can be harnessed to combat emerging threats and reduce operational business risks.

Speaker Info

First Name	Last Name	Company
Rob	Wainwright	Deloitte

Date: 1/10/2018

Time: 13:00 – 13:45

Track: Technology and Operations

The Real World of Threat Hunting: Tools, Tips, and Recipes

This session takes a deep dive into the world of threat hunting, common use cases and how to build a program. Learn how to leverage attributes and metadata of system-related activity to hunt for anomalous behavior; find the needle in the haystack and drill down into key events of interest; use threat intelligence appropriately when hunting across the enterprise; and take advantage of open-source tools for maximizing your forensic engagements.

Speaker Info

First Name	Last Name	Company
Tim	Bandos	Digital Guardian

Date: 1/10/2018

Time: 13:00 – 15:30

Track: Technology and Operations

STIX2/TAXII2 Workshop

This workshop will explore the new STIX/TAXII standards looking at a brief background on what changed and why, the interactive threat report modeling exercises using Python Jupyter notebooks; and how to use STIX2 to collaborate with teams using other languages.

Speaker Info

First Name	Last Name	Company
Chris	Ricard	FS-ISAC

Richard Struse MITRE OASIS

Date: 1/10/2018 **Time: 14:15 – 15:00** **Track: Technology and Operations**

Intelligent Threat Intelligence: Data Science at Scale

The current approach to assessing threat intelligence measures how good your data sources are, and the operational utility of this data. This is useful, and should be a part of any mature security practice. Instead, here we describe the effectiveness of the threat itself, and hence the amount of risk that a remediation mitigates. 299 CVEs are responsible for 44 million attacks. In the incident response paradigm, you can deal with 44 million attacks by monitoring and remediating around 30,000 malware samples, and see as those samples mutate and generate new strains. Or, you can remediate 299 CVEs, and never worry about those strands again.

Context and appropriate statistical blending of the data is what makes threat intelligence, well - intelligent.

Of the 8 trillion successful exploitation's over the past 4 years, 46,266,667 are attributed to 28,540 different malware samples. Even if you treat the pain of those 28,540 malware variants, the root cause remains. So let's treat the cause: Firstly, analysis of malware data lets you easily identify those vulnerabilities in your environment, and if they're high risk, we'll supply you with the MD5, SHA1 and SHA256 hashes to clean up the current infections. Root cause addressed. Second, if those 299 CVEs are assessed by volume and velocity of successful exploitation, one can easily see that only a handful of them are responsible for over 90% of the successful exploitation's. This granular prioritisation makes managing millions of incidents and tens of thousands of strains of malware less painful.

Speaker Info

First Name	Last Name	Company
Michael	Roytman	Kenna Security

Date: 1/10/2018 **Time: 14:15 – 15:00** **Track: Technology and Operations**

Top Cyber Risk Challenges Deception Can Help You Solve

When the topic of deception technology comes up, many people still think of honey pots—emulation systems used by skilled specialists for threat attribution. This presentation will provide a refresh on how deception has evolved in recent years to offer broader functionality across the cyber kill chain and more integral value within the risk-focused SOC. We'll look at how deception can address several especially persistent cyber challenges. In particular, we'll look at how deception can: fill important gaps in an insider threat program; provide an adaptive means of protecting critical assets during M&A transitions; help cut through noise in the SOC; uncover invisible cyber hygiene issues; and protect sensitive "untouchable" systems in situations where software cannot be installed.

Speaker Info

First Name	Last Name	Company
Ofer	Israeli	Illusive Networks

Date: 1/10/2018

Time: 15:15 – 16:00

Track: Threat Intelligence and Law

You Can't Always Get What You Want – Or Can You? More is Better in a Cloudy World

One of the challenges for financial institutions who are considering a move to the cloud is whether they will have the same level of controls for their data, infrastructure and threat management. This session will discuss new options in identity and access management, data protection and threat intelligence. Explore how real intelligence is now available from the oceans of data generated by the many endpoints and logs so that we can find needles and not just hay.

Speaker Info

First Name	Last Name	Company
Lisa	Lee	Microsoft Corporation

Date: 1/10/2018

Time: 16:15 – 17:15

Track: Human Element

Best Practices for Building an Insider Threat Program

The greatest cyber security threat an organisation 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, but whether unintentional or malicious, you need to quickly identify and eliminate insider threat. Attend this session to learn best practices for building and maintaining an effective insider threat program.

You will learn:

- Why insider threats are prevalent, despite many organisations implementing a layered defence approach
- How to stop insider threats in their tracks, through comprehensive visibility, real-time intelligence and policy enforcement
- How to help organisations achieve data privacy and protection compliance in line with GDPR regulations
- Why you need to focus on people, processes and technology, in that order.

Speaker Info

First Name	Last Name	Company
Simon	Sharp	ObserveIT

Date: 2/10/2018

Time: 08:30 – 09:30

Track:

PGP Key Signing Party

Join FS-ISAC members for a PGP Key Signing Party designed to share and validate PGP keys with your colleagues. Verify PGP keys in person and by signing a key you enable a higher level of trust between participants. If interested in attending please send ONLY your PUBLIC KEY to pgp@fsisac.com no later than Wednesday 25 September by 17:00 (UTC+2). Please note that you MUST physically appear in person and have two (2) forms of identification and at least one must be government issued, such as a national ID card, passport and/or driver's license. If you have never used PGP/GPG before or are having problems creating a key plan to join FS-ISAC staff on Tuesday 2 October during the breakfast from 0830 to 0930.

Speaker Info

First Name	Last Name	Company
John	Solomon	FS-ISAC

Date: 2/10/2018

Time: 09:45 – 10:15

Track: Threat Intelligence and Law

Is AI (Artificial Intelligence) in Cybersecurity the Solution?

Is artificial intelligence (AI) the solution to the challenges cyber-attacks pose to businesses everywhere? Go beyond the hype and explore real-world examples of AI algorithms. This session will cover anomaly detection, clustering, belief propagation, deep learning and more. Bust myths and learn the taxonomy of AI algorithms, what AI can and can't do, how to leverage AI as a preventative measure and best practices on incorporating AI into your threat detection and defense systems.

Speaker Info

First Name	Last Name	Company
Dr. Dhia	Mahjoub	CISCO

Date: 2/10/2018

Time: 10:15 – 10:45

Track: Threat Intelligence and Law

Moving Beyond Low-Level Indicators: Why Detecting Techniques is Where It's At

It's getting tougher to pin down the bad guys using low-level indicators like file hashes, domains and IPs thanks to adaptations in malware. Developing detections against these techniques can be time consuming. Fortunately, others have paved the way using common tools and logs. This session will show how to leverage the MITRE ATT&CK Framework for higher fidelity detections.

Speaker Info

First Name	Last Name	Company
Colby	Derodeff	Anomali

Date: 2/10/2018

Time: 11:15 – 12:00

Track: Technology and Operations

Mitre ATT&CK Framework Workshop

This session will discuss how to operationalise threat intelligence, evaluate your security posture and make decisions about your approach to cybersecurity using the MITRE ATT&CK Framework.

Speaker Info

First Name	Last Name	Company
Edward	Millington	Winton
Craig	Aitchison	Winton

Date: 2/10/2018

Time: 11:15 – 12:00

Track: Resiliency and Continuity

2017 Cyber Events and the Value of Regional and Global Trusted Information Sharing

Using real-life events like Petya malware attacks this session will assess a life cycle approach to information sharing. Using an anonymous interactive survey to gauge attendee experience with the malware and cyber-events of 2017 and share the sector viewpoint of information sharing these events. This session will also identify additional areas where information sharing would have increased the response capabilities or reduced the impact of the events as well as FS-ISAC research on information sharing boundaries and capabilities of the 2017 cyber threats and attacks.

Speaker Info

First Name	Last Name	Company
Susan	Rogers	FS-ISAC

Date: 2/10/2018

Time: 12:00 – 12:45

Track: Technology and Operations

Blockchain Security and Identity - Enablers for Broader Adoption

Eighty-percent of global executives expect blockchain technology to be integrated into their systems in the next three years. The time to begin thinking about risks, application development and its security implications, is now. Deciphering between the hype and reality of security threats to blockchain technology is a major first step. In this session learn how leveraging blockchain for security processes will help to enable a human-centric approach and reduce friction in our digital lives as well as how to increase efficiency, interoperability, manage our own identity data and reduce the need to build direct trust between systems.

Speaker Info

First Name	Last Name	Company
John	Velissarios	Accenture

Date: 2/10/2018

Time: 12:45 – 13:00

Track: Threat Intelligence and Law

Leadership in Crisis - Stories from the Range and Response

Leadership: it's not a new concept, but when looking at many of the major breaches in the last two years, it is apparent that the responses to such breaches cause more damage than the breaches themselves. This session will review lessons learned about human behavior and teach you how to lead your company through a crisis.

Speaker Info

First Name	Last Name	Company
Erno	Doorenspleet	IBM Security

Date: 2/10/2018

Time: 13:00 – 13:15

Track: Technology and Operations

Using "Magical Math" to Protect Cryptographic Keys

Learn how revolutionary breakthroughs in mathematics can allow secrets (cryptographic keys) to be used without ever being exposed, thus ensuring digital assets are safe – anytime, anywhere. At the heart of this lies the sophisticated applications of multiparty computation (MPC). Developed by world-renowned cryptographers, MPC offers a mathematical guarantee of security that fortifies disruptive technology. Join this session to learn how for the first time, trust-contingent operations are enabled anywhere, reaching far beyond the boundaries of physical infrastructure.

Speaker Info

First Name	Last Name	Company
Oz	Mishli	Unbound Technology

Date: 2/10/2018

Time: 13:15 – 14:00

Track: Governance, Risk, and Compliance

Building Cyber into the Credit Risk Model - Sizing Third-Party Cyber-Risk

An organisation's cyber-risk does not exist in isolation and can impact other operational and financial risks like liquidity, systemic, reputation and operational. This session will explore a technique for merging assessments of cyber-risk with an existing credit risk model, and the challenges and the benefits that it brings for both parties.

Speaker Info

First Name	Last Name	Company
Ben	Payne	Commercial Banking, Lloyds Banking Group

Date: 2/10/2018

Time: 13:15 – 14:00

Track: Threat Intelligence and Law

How Do You Look to an Attacker?

While financial services organisations have some of the most robust cybersecurity practices many still have publicly exposed assets that are unmanaged from a security perspective and pose a security and compliance risk. This session will look at common security exposures and compliance violations (including GDPR) across an average digital estate and the changes over time. As well as a discussion on how to automate and operationalise the oversight of assets exposed on the internet.

Speaker Info

First Name	Last Name	Company
Terry	Bishop	RiskIQ

Date: 2/10/2018

Time: 14:30 – 15:15

Track: Threat Intelligence and Law

TTPs Not IoCs: Using Threat Intelligence to Drive Threat Hunting

The baseline for effective security monitoring and detection has moved. While alert processing based on static information had been considered sufficient to identify threats, active threat hunting is now a core competency for SOCs. But, to hunt, you need to know how your quarry behaves and SOCs can't do this on their own. In this session learn how threat intelligence can detect threat actor behaviour by understanding tactics, techniques and procedures (TTPs).

Speaker Info

First Name	Last Name	Company
Andrew	Huddart	Bank of England

Date: 2/10/2018

Time: 14:30 – 15:15

Track: Governance, Risk, and Compliance

Disrupting the Disrupters: How Are We Doing?

With more than 1.2 million phishing threats detected in 2017, the financial industry is under constant attack. While ransomware has received the lion's share of attention last year, the everyday "beachhead" attacks were 2.5 times more prevalent. This session analyzes the phishing trends, attacks and defense strategies across the global financial sector. Join us to learn the latest threat and phishing attack data as well as how to compare benchmarking susceptibility and resilience to active phishing attacks.

Speaker Info

First Name	Last Name	Company
Jim	Hansen	Cofense

Date: 2/10/2018

Time: 14:30 – 15:15

Track: *Threat Intelligence and Law*

The State of Cyber: How Stealthier Attacks are Blurring the Lines Between Cybercrime and Statecraft

This session will shed light on alarming new trends CrowdStrike has observed in the global threat landscape, and the evolving best practices that are proving most successful against criminal, hacktivist and nation-state adversaries.

- The latest threat intel and predictions for 2018 and how you can use this to shape your security strategy
- Lessons learnt in the course of conducting in-depth digital forensics, IR and remediation with real-world strategic insight into the current threat landscape.
- How advanced attacks continue to succeed in evading modern defences
- How applied threat intelligence can deliver a decisive advantage in protecting your enterprise

Speaker Info

First Name	Last Name	Company
Zeki	Turedi	CrowdStrike

Date: 2/10/2018

Time: 15:30 – 16:15

Track: *Governance, Risk, and Compliance*

Industry Initiatives for Enhancing EU and International Cyber Threat Response Harmonisation and Effectiveness

EU initiatives are in progress to strengthen EU's cyber preparedness and deterrence, but will it be enough for firms to prepare, respond and recover from current and future threats? This session will explore a variety of topics on how to harmonize the EU and international threat response capabilities. Cyber is a global issue that needs stronger international cooperation.

Speaker Info

First Name	Last Name	Company
Emmanuel	Le Marois	AFME

Date: 2/10/2018

Time: 15:30 – 16:15

Track: *Testing and Security Assurance*

Insights into Cyber Assurance Testing

Independent reviews of cyber controls and capabilities are fundamental in the overall security strategy for an organization. Join this session to discuss what insights can be gained from evaluating cyber-assurance testing methodologies like red team testing, education, awareness and cyber-assurance exercises.

Speaker Info

First Name	Last Name	Company
Marco	Lazzari	UBS
Carlo	Hopstaken	UBS

Date: 2/10/2018

Time: 15:30 – 16:15

Track: Technology and Operations

Threat Mosaic: Using Threat Intelligence to Improve Collaboration and Communications

Most organizations are now leveraging threat intelligence in one way or another. The question is whether they are using it the “right” way to make use of all their people, process and technology with an eye toward stake holders. This session will walk through how a threat mosaic is created from security collaboration and how your threat knowledge base can be leveraged to communicate business-critical information to executives, the board, business units and other security teams.

Speaker Info

First Name	Last Name	Company
Jonathan	Couch	ThreatQuotient

Date: 2/10/2018

Time: 16:30 – 17:17

Track:

CISO Panel

Join four FS-ISAC Member CISOs as they discuss top of mind issues facing our industry. Participants will be contributors from Europe, including representatives from banking and insurance firms. Each year this session is a highlight of the summit, be sure to be there and hear what the leaders of our industry are working on!

Speaker Info

First Name	Last Name	Company
------------	-----------	---------

Date: 3/10/2018

Time: 09:30 – 10:30

Track: Threat Intelligence and Law

Fighting Cybercrime-as-a-Service by Understanding its Economics

While cybersecurity vendors try to estimate the global economic impact of cybercrime and use those figures to elevate their commercial pitch, the reality shows that the quick adoption of new technologies by cybercriminals and the increased ease of committing cybercrime has built up the perfect storm for the growth of cybercrime-as-a-service (CaaS) against financial institutions. In this session take a deep-dive on what kind of CaaS detected in the last months from a FI perspective, distinguishing its profitability, actors profiling, CaaS incubators "driven by opportunity", geographical distribution and an analysis of six months of CaaS. Finally, learn how to tackle CaaS not in FIs perimeters but by understanding the economics beyond it to define new initiatives to stop it.

Speaker Info

First Name	Last Name	Company
Adolfo	Hernandez	Banc Sabadell

Date: 3/10/2018

Time: 10:45 – 11:30

Track: Threat Intelligence and Law

Analyzing and Applying FS-ISAC Reporting to a Threat Intelligence Program

This workshop will demonstrate how to analyze FS-ISAC reporting and apply it to your threat intelligence program. A simple methodology without the need for costly tools will help threat analysts understand how to identify trends and emerging threats. By capturing the indicators of compromise and monitoring for their presence in internal telemetry systems, one can identify if being targeted with the same campaigns observed by peers.

Speaker Info

First Name	Last Name	Company
Emma	Fahy	Fidelity Investments

Date: 3/10/2018

Time: 10:45 – 11:30

Track: Technology and Operations

SOC-CMM & MaGMa UCF: Tools for Effective Cyberdefence

This session will explore the Security Operations Center Capability Maturity Model (SOC-CMM) and the Management, Growth, Metrics & assessment use case framework (MaGMa UCF), two free tools that can enhance cyberdefence. Learn about the SOC-CMM a self-assessment tool that is used to measure SOC capability maturity across five domains - business, people, process, technology and services on a five-point scale. Then hear about the MaGMa UCF, a framework for use case management that was created as a joint effort with the Dutch financial security community (FI-ISAC). Effective cyberdefence can happen with the right tools.

Speaker Info

First Name	Last Name	Company
Rob	van Os	Volksbank

Date: 3/10/2018

Time: 10:45 – 11:30

Track: Threat Intelligence and Law

Black Swans and Threat Horizon Scanning

Strategic threat horizon scanning is growing in importance and has an important role to play in financial organisations today. Strategic reports and predictions are made, but often they prove to be inaccurate and miss a major development. 'Black Swans' can often float down the river into our environment and upset our plans. This session will explore how to hunt for the unknown threats. What methods and approaches have helped? What can be used to better inform strategic threat predictions and reports? What will be voted on the top threats of 2019?

Speaker Info

First Name	Last Name	Company
Dr. David	Aubrey-Jones	Royal Bank of Scotland

Date: 3/10/2018

Time: 11:45 – 12:30

Track: Technology and Operations

Agile Security Engineering and Evidence on Demand

Agile Security Engineering (ASE) is a new way of working for the Information Security Officers (ISO) within Rabobank to align our Waterfall based System Security Risk Management process more to the Agile delivery process of our IT Teams. Via ASE we become part of the process of delivering new features and thereby give security ownership back to the teams. In this session I will share our journey from Waterfall Security Management towards Agile Security Engineering and provide a best practice currently used for multiple Agile teams within Rabobank.

In the discussion I would like to focus on how you align your IT Asset Security Management process to the Agile world. How do you stay in control during continuous development and having updated applications every 3 weeks? What competence's/knowledge do you require the ISO's to have so that they can engage with Agile delivery teams. Plus envision "Evidence on Demand" what data do you need to have a live security status of your IT landscape?

Speaker Info

First Name	Last Name	Company
Alex	Duivelshof	Rabobank

Date: 3/10/2018

Time: 11:45 – 12:30

Track: Threat Intelligence and Law

Insurance-Sector Threat Intel and Best Practice Exchange

Members only, TLP red session on optimal metrics, insurance-specific threats and TTPs, threat intel innovation, security orchestration and automation, sector intel sharing and more!

Speaker Info

First Name	Last Name	Company
Christopher	Guy	Swiss Re

Date: 3/10/2018

Time: 13:30 – 14:15

Track: Resiliency and Continuity

Review of FS-ISAC's 2018 EMEA CAPS Exercise Results

This presentation will review results from the participants of the 2018 Cyber-Attack Against the Payments System (CAPS) Exercises in EMEA and Asia-Pacific. Hear aggregate responses from the regional incident response teams, ask for feedback on the 2018 exercise and request content for the 2019 CAPS exercise.

Speaker Info

First Name	Last Name	Company
Charles	Bretz	FS-ISAC

Date: 3/10/2018

Time: 13:30 – 14:15

Track: Governance, Risk, and Compliance

Information Sharing Community Participation Maturity (ICPM) - Workshop

In this session hear from the ICPM on who they are and what has been achieved so far. Learn about the information sharing maturity model; topics and questions for a member survey; and self-assessment approach and metrics.

Speaker Info

First Name	Last Name	Company
Tania	Brown	Deutsche Bank

Date: 3/10/2018

Time: 14:30 – 15:15

Track: Resiliency and Continuity

Demo of a Cyber-Range Exercise

Join us for a high-level overview of how cyber-ranges work and the use cases for them. Discuss overall sector program, plans for international support and lessons learned so far from our new cyber-range series.

Speaker Info

First Name	Last Name	Company
Greg	Gist	FS-ISAC

Date: 3/10/2018

Time: 14:30 – 15:15

Track: Threat Intelligence and Law

Bring Your Own Intelligence

Want to talk to your peers about threats and what they are seeing? This TLP RED roundtable session will give you the opportunity to discuss various issues, share what you know and learn what is happening around the region. Be prepared to provide a snapshot of your top threats and concerns! Active Participation REQUIRED

Speaker Info

First Name	Last Name	Company
Teresa	Walsh	FS-ISAC

Date: 3/10/2018

Time: 15:30 – 16:15

Track: Technology and Operations

GNU Taler

Join this session for a demonstration of GNU Taler an online payment system that uses Chaum's blind signatures to provide robust privacy for customers along with accountability for merchants and payment service providers, as well as a discussion of integrating the merchant software into existing web sites. Hear from the Internet Engineering Task Force (IETF) on a standardize a URI, schema for payments (payto://) and an outline how the Taler protocol accomplishes goals such as giving change and refunds.

Speaker Info

First Name	Last Name	Company
Christian	Grothoff	Bern University of Applied Sciences

Date: 3/10/2018

Time: 15:30 – 16:15

Track: Governance, Risk, and Compliance

Cloud Security Awareness Game

Join this session to experience a cloud security awareness game to learn about cloud security risks and improve the quality of risk assessments. First-come, first-served.

Speaker Info

First Name	Last Name	Company
Olaf	Streutker	ABN AMRO Bank
Jim De	Haas	ABN AMRO Bank
Gerrit	Bierhof	ABN AMRO Bank
Nadine	Lamotte	ABN AMRO Bank