FS-ISAC

2020 Europe Virtual Summit
Summit Agenda

Agenda subject to change

Wednesday 4 November 2020 - All Times are UTC/GMT

09:00–10:00 **Virtual Solutions Hall Open**

10:00–11:00

OPENING REMARKS: Steven Silberstein, CEO, FS-ISAC; Jerry Perullo, CISO, ICE, Board Chair; *Ramy Houssaini, CSO, BNP Paribas, Summit Chair*

KEYNOTE: The Future of the Criminal Underground: Dark Web Sneak Peek
Janey Young, Europol EC3

Privacy orientated software is a key enabler of crime in the modern world. It provides criminals with shadows in which to hide, perfect platforms of anonymity to commit illicit trade and support crime and terrorism. This session will introduce the murky world of the dark web, highlighting the scope of the threat. It will outline the international law enforcement strategy to tackling this, including the partnerships and collaborations in place. Lastly, it will identify the challenges going forward and provide a forecast for the future of the dark web.

11:00–11:15 **Virtual Solutions Hall Networking Break**

11:15–12:00
General Sessions

A Journey Towards Threat-Centric Security
Sanjeev Shukla, UK & Ireland Financial Services Security Lead, Managing Director, Accenture
Carsten Fischer, Managing Director, Chief Security Office (CSO), Global Head Information Security Operations (ISO), Deutsche Bank

- Understand the complementary nature of compliance goals and protection against threats
- Demonstrate a sustainable framework for your threat-centric security journey
- How to leverage existing investments

Eat. Sleep. Phish. Repeat.
Zeki Turedi, CTO, Europe, Middle East and Africa, CrowdStrike

- Recommendations for protecting your organisation's data and network across both corporate-supplied and employee-owned devices, regardless of their location
- Today's attack trends and who is being targeted, including a review of key examples
- What can be done to combat the continued rise of ransomware that leverages the fear and uncertainty around the pandemic
- Latest findings from the 2020 OverWatch report, including analysis of key adversary activity

FS-ISAC

2020 Europe Virtual Summit
Summit Agenda

Agenda subject to change

Wednesday 4 November 2020

11:15–12:00
General Sessions
Continued...

IOC You Now – Automated Needle Finding At Scale
Richard Cassidy, Senior Director, Strategy. Exabeam; Jan Willekens, Product Owner of Cyber Defense Center, Swedbank

What can attendees expect to learn?

- Challenges and limitations of logging and querying when searching for IOCs at scale - from people, process, and technology perspectives
- How to effectively automate the usage of IOCs and threat intelligence data
- How to measure automation success in terms of both security and business risk

12:00–12:45 **Lunch and Virtual Solutions Hall Networking**

12:45–13:15
Concurrent Sessions

Fraud/Cloud

Ransomware Response - Best Practices
Jerry Bessette, SVP Incident Response, Booz Allen Hamilton
Anthony Harris, Principal/Director, Incident Response, Booz Allen Hamilton
Greg Baker, Senior Associate, Ransomware Negotiations, Booz Allen Hamilton

- An overview of the most prolific ransomware threat actors
- Concrete recommendations on building an effective response plan
- A discussion of negotiation best practices and ‘not so’ effective practices
- Recommendations for leveraging existing tools and technology to become more resilient against ransomware attacks

Governance Risk & Compliance

What to Expect When Expecting a Pen Test
Tony Drake, Senior Engineer, Information Security Intelligence, ICE/NYSE

- What a pen test is
- What a pen test is not
- How to get a better pen test
- How to deal with pen test results

Wednesday 4 November 2020

12:45–13:15 Concurrent Sessions Continued...	**Advanced Technologies & Techniques**	**How Real-Time Collaboration During COVID-19 Saved the Day** *Gavin Landless, VP Risk Management, Empower Federal Credit Union* *Steven Wallstedt, Head of Information Security and Business Continuity, ABN AMRO Holdings USA LLC* • The benefits of real-time, peer-to-peer chat during a crisis • What the response to COVID-19 looked like for small and large financial institutions • How organizations can better prepare for black swan events in the future
13:15–13:30	**Networking Break**	
13:30–14:00 Concurrent Sessions	**Fraud/Cloud**	**Building a Threat Hunting Programme** *Francois Cappellen, Head of Threat Hunting, SWIFT* To overcome some of the downsides of the focus on detection, in early 2020, SWIFT started a new programme evolving the Threat Hunting practice from ad-hoc hunting on very specific TTPs towards a repetitive activity integrated with the role of the Cyber Fusion Centre. During this session, we will highlight reasons to develop such a programme, some of the pitfalls, and some of the achievements to date.
	Governance Risk & Compliance	**Systemic Cyber Risk: In Theory and Practice** *Harriet Gruen, Cyber Risk Specialist, Tokio Marine Holdings* *Tinglin Huang, Cyber Data Analyst, Tokio Marine Holdings* • A high-level overview of approaches for modelling systemic cyber risk • Using scenarios to identify areas of exposures and dependencies • Data collection and modelling approaches when looking at systemic risk • Transferable lessons learned: e.g. for supply chain mapping and reviewing client exposures

FS-ISAC

2020 Europe Virtual Summit
Summit Agenda

Agenda subject to change

Wednesday 4 November 2020

13:30–14:00 Concurrent Sessions Continued...	**Advanced Technologies & Techniques**	**Understanding the Ransomware Landscape** *Ippolito Forni, Senior Threat Intelligence Analyst, EclecticIQ* • Contextual understanding of malicious ransomware and its evolution • Learn common modi operandi of ransomware threat actors and common ransomware operations tactics, techniques, and procedures • Ransomware prevention and response via CTI-driven security: leveraging strategic, operational and tactical intelligence • If your organization becomes a victim: steps that can be taken to avoid paying the ransom, or, negotiation tips if the payment is the only option.
14:00–14:30	Networking Break in Virtual Solutions Hall	
14:30–15:00 Concurrent Sessions	**Fraud/Cloud**	**Application Security Beyond Effective Bot Mitigation** *Larry Venter, RVP Solutions Engineering, Shape Security part of F5* • Defeat digital fraud - how to separate fake users from your real customers • Reduce friction and improve customer experience • Increase digital engagement and improve conversion rates
	Governance Risk & Compliance	**6 Steps to Streamline Third-Party Financial Due Diligence & Business Continuity** *Scott Bridgen, Head of GRC, OneTrust* • Learn how organizations are handling current market disruptions • Overview of streamlining rapid supplier financial due diligence • Developing and executing third party business continuity plans
	Advanced Technologies & Techniques	**Adversarial DevOps and Red Team Infrastructure** *Carel van Rooyen, Head of Red and Purple Team Operations, Swiss Re;* *Sven Bernhard, Senior Red Team Tester, Swiss Re* • Why operations require replicable, segregated infrastructure • Being able to describe the benefits of testing deployment states • Logging and monitoring ELK (Elasticsearch, Logstash, and Kibana) stacks for deconfliction

FS-ISAC

2020 Europe Virtual Summit
Summit Agenda

Agenda subject to change

Wednesday 4 November 2020		
15:00–15:15	Networking Break	
15:15–15:45 Concurrent Sessions	**Fraud/Cloud**	**How to Stay Ahead of Threats in a Global Pandemic** *Richard Meeus, Security Technology and Strategy Director, Akamai* *Gerd Giese, Strategist, Financial Sector, Akamai* • Global view of a global pandemic and how to digitally survive the next one • Implementing the shift to a remote workforce and smarter access • How to be a leader for security and user experience
	Governance Risk & Compliance	**Threat Trends: The Evolution of Metrics Led Intelligence** *Jo Kleiman, Intelligence Collection Manager, FS-ISAC* • Understanding of FS-ISAC's metrics program: purposes and goals • Renewed appreciation of the importance of proactively sharing intel • Resources and advice on safe and trusted threat data sharing
	Advanced Technologies & Techniques	**Lessons Learned: "Threat Hunting & Purple Teaming"** *Anders Sand Frogner, Security Analyst, DNB* • Why you should do Threat Hunting and Purple Teaming • Practical examples of Threat Hunting and Purple Teaming • Getting started, expected results and measurements

Thursday 5 November 2020 - All Times are UTC/GMT	
09:00–10:00	**Virtual Solutions Hall Open**
10:00–11:00 General Session	**OPENING REMARKS** **Ray Irving, Managing Director – Global Business, FS-ISAC;** *Ramy Houssaini, CSO, BNP Paribas, Summit Chair* **Information is What I Want, Knowledge is What I Need** *Stefano Ciminelli, CISO - Group Head of Cybersecurity, Unicredit* • Sharing information is important, sharing knowledge makes all the difference • The security industry and media gives hard times to victims of cyberattacks - but the life of defenders is really hard • Why are we not more effective in sharing information among organizations? • Regardless of how complex your intelligence technology stack is, the real difference is made by individuals and their own network
11:00–11:15	**Networking Break**

Thursday 5 November 2020

11:15–11:45 Concurrent Sessions	**Fraud/Cloud**	**Getting your Board on Board with Collective Defense and How to Implement** *Brett Williams, Co-Founder & Chief Operating Officer, IronNet Cybersecurity* • How to apply the foundations of a Collective Defense approach across your organization to strengthen your cyber defense • Ways to use behavioral analytics to improve detection of unknown, sophisticated threats by criminal and nation-state adversaries • Factors for building the business rationale of investing in Network Detection and Response and Collective Defense for better cybersecurity protection of your entire business ecosystem, including third-party vendors
	Governance Risk & Compliance	**Purple Team Operations Year One** *Carel van Rooyen, Head of Red and Purple Team Operations, Swiss Re* *Philipp Promeuschel, Expert Security Engineer, Swiss Re* • Automation is key in providing red/blue collaboration platforms • Optimisation of time and security: code integration is best handled with a predictable cadence of operations • Recommendation of communication and reporting for trends in engineering rather than pure gap analyses • Advising on ROI-optimisation in operations
	Advanced Technologies & Techniques	**Getting Intelligence Right Delivering Trustworthy Intelligence by Operationalizing the Intelligence Cycle** *Freddy Murre, Senior Threat Intelligence Analyst, NCE* • What is Intelligence and how it can be operationalized in cyber threat intelligence • What is the Intelligence Cycle and how it can help structure intelligence production • Helping stakeholders understand the Intelligence production process and how to use a finished product to their advantage
11:45–12:00	**Networking Break**	

FS-ISAC

2020 Europe Virtual Summit
Summit Agenda

Agenda subject to change

Thursday 5 November 2020

12:00–12:30 Concurrent Sessions	**Fraud/Cloud**	**Scale Up to Your Security Telemetry** *Chris Martin, Senior Security Specialist, Google Cloud Security* • Understand what to do with your increasing amounts of security telemetry data • Learn how to investigate threats and attacks within your own network at the speed of a Google search • Use security analytics as a force multiplier for threat hunting and incident response
	Governance Risk & Compliance	**Technology Enablement in the Intelligence Cycle and the Role of TIPs** *Andreas Sfakianakis, Threat Intelligence Lead EMEA, S&P Global* • TIP as a central role in CTI analyst's toolset (not necessarily a single pane of glass) • Use of diverse technology to support cyber intelligence and monitoring the emerging technology • Selecting toolsets based on YOUR requirements and use cases • How to build technology around processes and not the other way around • Adopting SOAR capabilities for workflows, automation and threat analysis playbooks • Helping the community and working effectively with vendors
	Advanced Technologies & Techniques	**Malware in the Time of COVID** *Lisa Lee, Chief Security Advisor/Global Lead for Financial Services, Microsoft* • Recent attack-type trends • Immediate actions for prevention and preparedness • Longer-term defense measures and coordinated defense against complex attacks
12:30–13:15	**Lunch and Virtual Solutions Hall Networking**	

Thursday 5 November 2020

13:15–13:45 Concurrent Sessions	Fraud/Cloud	**Mitigating Risk by Enabling the Human Facto** *Jelle Wieringa, Security Awareness Advocate for EMEA, KnowBe4* • Find out how security awareness training combined with frequent simulated phishing can help improve organisational security • Learn how to combine psychology insights with human behavior to create a successful security awareness training program • Learn the differences between security awareness and security behavior and how to use the distinction to your advantage
	Governance Risk & Compliance	**Leveraging Data Analysis to Enhance Vendor and Open-Source Threat Feeds** *Karen Lamb, Lead Cyber Intel Analyst, HSBC* *Colin Martin, Cyber Intelligence Principal Analyst, HSBC* • Review of issues arising from failure to adequately label data • Overview of off-the-shelf tools for conducting this analysis and of custom techniques for comparing IoCs • Use case: applying this analysis to improving a vendor threat feed and expanding our own intelligence collection capabilities • Better understanding how to leverage these data analysis techniques against your own threat data
	Advanced Technologies & Techniques	**Increasing Detection and Mitigation Maturity through Internet Visibility** *Terry Bishop, VP Technical Services, EMEA, RiskIQ* • Viewing frameworks such as Lockheed Martin Cyber Kill Chain®, F3EAD and MITRE ATT&CK from a new perspective to improve existing defence programs • Understanding how Internet intelligence can improve the frameworks' early stage effectiveness • Illustrating the above through live reconnaissance data on organisation and threat actor infrastructure
13:45–14:00 p.m.	**Networking Break in Virtual Solutions Hall**	

FS-ISAC

2020 Europe Virtual Summit
Summit Agenda

Agenda subject to change

Thursday 5 November 2020

14:00–14:30 Concurrent Sessions	**Fraud/Cloud**	**The Life of a Trade from an InfoSec Prespective - EMEA Edition** *Peter Falco, Director, FS-ISAC;* *Jenny Mannent, Senior Expert Markets and Infrastructure, Swedish Securities Markets Association* • Enhanced understanding of the importance of a securities trade • Protecting the entire trade life cycle • Risks involved in reporting a trade
	Governance Risk & Compliance	**Collective Defense Through End-to-End Automation of Bi-Directional Threat Intelligence Sharing** *Neal Dennis, Threat Intelligence Specialist, Cyware; Jake Smith, Solutions Architect, Cyware* • How end-to-end automation can enhance intelligence sharing • How real-time collective defense can be achieved in continuity by automating threat intelligence sharing • How to determine priority and relevancy for smarter intelligence actioning
	Advanced Technologies & Techniques	**Incident Response for the Unprepared, Overwhelmed, and Understaffed** *Tony Drake, Senior Engineer, Information Security Intelligence, ICE/NYSE* • Understanding the human factors of incident response • Understanding planning and executing incident response • Understanding tools and techniques incident response, even without corporate tools
14:30–14:45	**Networking Break**	
14:45–15:30 Concurrent Sessions	**Open Banking and PSD2: Open Doors and New Threats** *Dr. David Aubrey-Jones, Threat Readiness Team Leader, Natwest Group* • An understanding of Open Banking and the changes it brings. • Threats of Open Banking and how these may be exploited. • Open Banking issues and additional security measures to consider.	
5:00 p.m.	**Summit Concludes**	

On-Demand Sessions

These thought leader sessions will be available for On-demand streaming during the entire event. Attendees may download and watch the following sessions during the two virtual summit days and receive points on the leaderboard.

- Achieving Least Privilege in the Cloud | **Amazon Web Services**
- Actively Defending the Enterprise: Segmentation Strategies for Sustainable Outcomes | **ForeScout Technologies**
- Addressing Application Resilience in Today's Complex, Dynamic Environments | **vARMOUR**
- Architecting to Successfully Embrace AI/ML Security | **Endace**
- CCM: Gartner's New Risk Management Category: The 'what' and 'why' | **Panaseer**
- Effective Fraud Prevention - It takes a Village | **Pindrop**
- Everything-as-a-Service: Trends in the Cybercrime Financial Ecosystem (and How Can Defenders Exploit Them) | **KELA**
- Extreme Makeover: AppSec Edition | **NetSPI**
- Looking Past the Pandemic: Futureproofing Against Data Risk | **Microsoft**
- Next Generation Software Security Initiatives | **Synopsys**
- Payment Platform Fraud on the Darkweb | **Sixgill**
- Preparing for a Breach - The Cybercriminal Perspective | **IntSights Cyber Intelligence**
- Put Zero Trust in Your Devices | **Eclypsium**
- Synthetic Identity Fraud - Caught in the Act | **Incognia**
- The Critical Need for Cyber-Resilient Systems | **Attivo Networks**
- The Dark Sisde of 3rd Party Scripts | **Source Defense**
- The Maturing of Compromise from BEC to EAC | **Proofpoint**
- Top 5 Threat Hunting Best Practices | **Reversing Labs**
- Understanding Open Source Risk | **Veracode**