BORDERLESS CYBER
EUROPE 2016

8-9 September
Brussels, Belgium

Programme Agenda

THURSDAY, 8 SEPTEMBER

9:00-10:00—Morning Plenary Session

Welcome Remarks

Conference Chair: Freddy Dezeure, Head of CERT-EU

What You Don't Know Can Harm You

Plenary Guest Speaker: Merike Kaeo, CTO, Farsight Security

The last year has seen a tremendous amount of global collaboration to bridge the gaps that were barriers to timely sharing of threat intelligence data. Cohesion across technical, operational and policy boundaries now provide actionable frameworks to create policies and contracts that can then be translated to the technical details needed to instrument automated realtime information sharing. If you don't know latest developments for breaking barriers in information exchange then you are losing out on information that could be helping you deter attacks and protect yourself from harm. The audience will hear firsthand the latest developments from the FIRST community Information Exchange Policy (IEP) work and the collaboration with OASIS along with other efforts underway to increase timely action and response from both the government and private sectors.

10:00-10:30—Session Block

Different Steps for Dealing with Cyber Attacks on a Country Level: Do's and Don'ts …

Presenter: Miguel De Bruycker, Managing Director, The Centre for Cybersecurity (CCB)

Security management can be a tedious job. Whether you are the chief information officer (CIO), chief technology officer (CTO) or even the chief executive officer (CEO), it can be hard to deal with possible risks and apply appropriate controls. In this presentation, the director of the Center for Cybersecurity Belgium (CCB) will share his real-world experiences in dealing with a major cyberattack. He'll discuss lessons learned during the different stages of the act, as well as the new measures and processes in inserted to help discourage countries, organizations and individuals from launching future cyberattacks.

10:30-11:00—Refreshment Break

11:00-11:30—Session Block

Clearing the Hurdles to Realize the Value of Threat Intelligence: IOCs, TTPs, and Sharing Organizations in Critical Infrastructure

Presenter: Chris Blask, Executive Director, ICS-ISAC

Following many recent initiatives, ICS-ISAC Chief Executive Officer, will share information on how his organization teamed up to create a platform for critical infrastructure operators worldwide to share threat data. With so many trusted technology partners, indicators of compromise and sharing organizations involved in the threat intelligence community, it was obvious many hurdles would play a role. Mr. Blask will provide details on those various hurdles and how the path was cleared. Part of the discuss will involve incorporating the use of real-time, machine-readable threat intel feeds via the STIX (Structured Threat Information Expression) and TAXII (Trusted Automation Exchange of Indicator Information) protocols.

11:30-12:00—Session Block

Building an Efficient Incident Response Process Using Threat Intelligence

A Global Enterprise Perspective

Presenter: Thomas Schreck, Senior Engineer, CERT -Head of the Incident Response Team, Siemens AG

During this presentation, Thomas Schreck from Siemens CERT will open up by providing an overview of the efforts and challenges experienced while working for a large global company where IT plays a key role in every area. The discussion will include details on building an efficient incident response process using threat intelligence by way of a combined strategy containing reactive and proactive services, as well as plan for long-term resilience. Key factors mentioned will be the need for a good team with support from automated processes.

12:00-12:30—Session Block

Financial Sector Use Case featuring Cyber Threat Intelligence Processes & Sources

Presenter: John Carlson, Chief of Staff, FS-ISAC

Experts expect increasingly sophisticated cyberattacks to continue, with the financial industry as a prime target. Beyond the impact to an individual bank, cyber risks have far-reaching economic consequences. To adequately deal with the persistent threat, the industry has come together to collaborate, identify weaknesses, and share industry standards and best practices. Much can be learned from their experiences. In this session, FS-ISAC Chief of Staff, John Carlson, will provide guidance on ways to implement a comprehensive cybersecurity information sharing system that will help you make a positive step toward better protecting consumers and the economy as a whole.

12:30-14:00—Luncheon

14:00-14:30—Session Block

If It’s Worth Sharing, It’s Worth Sharing Right— Technical, Policy and Legal Considerations of Cyber Threat Intelligence Sharing

Presenter: Richard Struse, Chief Advanced Technology Officer, National Cybersecurity and Communications Integration Center (NCCIC), U.S. Department of Homeland Security

The discussion around sharing cyber threat information (CTI) has evolved over the years from “can we / should we?” to “how?” This evolution has many drivers including the changing threat landscape, new legislation (including the CISA of 2015 in the U.S.) and the increasing number of mature, capable information sharing & analysis organizations (ISAOs). This presentation is intended to help individuals and organizations that have decided to share cyber threat intelligence do so in as an effective manner as possible by examining the technical, policy and legal implications of CTI sharing, based on real experiences and lessons learned. The goal is to help the audience understand the various challenges they may face in their own environments and learn from trusted partners who have already tackled similar issues.

14:30-15:45—Session Block

A New Security Dimension Roundtable: Industry Experience Using STIX, TAXII, and CybOX to Accelerate Threat Response

Moderator: Ivan Niccolai, Head of Asia Pacific Operations & Lead Analyst, KuppingerCole
Presenters:
Joep Gommers, Founder & CEO, EclecticIQ
Daniel Riedel, CEO, New Context, Inc.
Jason Keirstead, Product Architect-IBM Security QRadar, IBM Security Intelligence
Alex Valdivia, Senior Threat Intel Research Engineer, ThreatConnect, Inc.
Frank Lange, Principal Security Architect, Anomali

As we’ve heard, it is becoming increasingly necessary for a broad range of organizations to have a cyber threat intelligence capability. A key component of success for any such capability is information sharing opportunities with the partners, peers and others they elect to trust. Voluntary information sharing can help focus and prioritize the use of the immense volumes of complex cyber security information available to organizations today. Standardized, structured representations of this data make it tractable. The STIX language is meant to convey the full range of cyber threat information and strives to be fully expressive, flexible, extensible, automatable, and as human-readable as possible, while relying on relatively simple toolsets. But what does it take to make structured info sharing an operational reality? This session will describe operational implementations and real-world lessons learned from key implementers.

15:45-16:15—Refreshment break

16:15-16:45—Session Block

Best Practices in Information Sharing Across Governments, SMEs, and Vertical Communities

Presenter: Alexandre Dulaunoy, Security Researcher, Computer Incident Response Center Luxembourg-CIRCL

As we know security incidents are not restricted to specific geographical locations or administrative boundaries. Security experts from all different backgrounds at the Computer Incident Response Center Luxembourg (CIRCL) are working together to develop and share best practices, tools, methodologies, processes and trusted communications fitting for many different industries. During this session, Alexandre Dulaunoy--a Security Researcher from CIRCL, will share some of their findings and recommendations. Sharing information and best practices across different domains will further our worldwide message that strong collaboration between security teams and outstanding expertise are key components to successfully combating further threats.

16:45-17:00—Closing Session

Final Daily Remarks

Conference Chair: Freddy Dezeure, Head of CERT-EU

FRIDAY, 9 SEPTEMBER

9:00-10:00—Opening Session

Morning Remarks

Freddy Dezeure, Head of CERT-EU

Keynote Address: Recent EU actions on cybersecurity in particular around NIS and the cPPP

Andrus Ansip, Vice-President for the Digital Single Market, European Commission

10:00-10:30—Session Block

Breaches & Boardrooms: Bringing cyber to the C-level and keeping it there

Presenter: Dirk Lybaert, Chief Corporate Affairs Officer and former Secretary General, Proximus

Cyber security is a key enabler and an absolute necessity for the digital economy. Governments, citizens, organisations and enterprises need to build trust in the new digital way of life in order to bring our economy in a new prosperous era. Proximus as telecom operator is an innovator and crucial actor in this new digital value chain. That's why cyber security is at the core of our business and our daily preoccupations. Cyber security isn't just an IT problem anymore, it is a company-wide issue that must be managed across the whole organization. To get it effective, cyber security must be directly handled at the top of the organization. Involvement of the Board and Executive Committee is key success factor to ensure cyber security gets the right priority and resources in the organization, and especially that it is aligned with the business strategy and is enabling the business transformation.

The presentation will address such topics as:

- What boosted cyber to the C-level ?
- It is not anymore an IT problem only… it is a company-wide issue
- Cyber program : a company transversal approach
- Getting visibility and active involvement at C-level
- Approaching cyber risk management from a business perspective
- Enabling business transformation

10:30-11:00—Refreshment Break

11:00-11:30—Session Block

The Business of Battle Readiness: Over-the-Horizon Threat Management for Companies and Agencies

Presenter: Roland Cloutier, SVP, CSO, ADP Worldwide Services

In an age of business operations protection requirements that span global geographies and jurisdictions for Non-Government Operations, noted author and Staff Vice President, Chief Security Officer for ADP, Roland Cloutier, will provide innovative insights to how companies must utilize over-the-horizon planning, intelligence, and resource alignment to ensure the protection of the operating entities they are responsible for. From integrated commercial and public-private intel sharing to advanced threat analysis and automated defensive controls architectures, Roland will discuss new approaches and services that create leveraged resource enablement and threat management, providing a new level of readiness for today's cyber defenders.

11:30-12:30—Session Block

Cyber Threat Intelligence Information Sharing Collaboration Roundtable: Increasing Awareness of Vulnerabilities, Incidents, & Mitigations

Moderator: Paul Timmers, Director of the Sustainable & Secure Society Directorate, European Commission

Presenters:

Ian West, Chief, Cyber Security , NATO C&I Agency

Paul Chichester, NCSC UK

Hans de Vries, Head of National Cyber Security Centre (NCSC)

Recent cyber-attacks and widely reported pervasive vulnerabilities highlight the rapidly changing cyber risk landscape. Participating in collaborative information-sharing activities has been known to improve your ability to identify attack tactics and successfully mitigate cyber-attacks. During this panel session, industry leaders will offer insight to how they're navigating threats using information sharing techniques. Attendees will learn how each is identifying vulnerabilities with actionable remediation recommendations, enabling proactive mitigation to exploitable risks and plans underway to adopt best practices in incident response.

12:30-14:00—Luncheon Break

14:00-14:30—Session Block

IT Security @ Volkswagen

Presenter: Beate Hofer, CISO, Volkswagen

As our security landscape evolves, with each new threat comes an even stronger need to work together in order to stay ahead of malicious actors. While boards have traditionally been focused on guiding their organizations to maximizing shareholder value, the strain of such breaches is gaining prominence at their level. Ensuring their organization leverage information to establishing sustainable approaches for managing risk and reducing the likelihood of becoming the next breach, is now a primary mandate for CISOs. Volkswagen's CISO will provide insight on how her company is working to enhance collaboration techniques in an effort to build sufficient policy compliance, and high-risk plans that address the needs for higher level controls.

14:30-15:00—Session Block

Can You report to Your Board on Cyber Security with One Single Indicator? Approach for CISOs to Measure and Report Risk & Maturity on a Group Level

Presenter: Jan Nys, General Manager, Information Security & Infrastructure Architecture, KBC Group

With the relentless evolution of cyber security threats, today's leaders are prompted to evolve plans and deal with them more and more at the C-suite level. With many top level managers still viewing cybersecurity as too technical an issue to manage at an executive level, a specific approach is needed to effectively assist them. During this session, the speaker will provide his insight from a company operating in different countries with strong local commercial focus and accountability. He'll share a cyber risk management approach that enables you to prioritize all the different aspects of your cybersecurity program, so you can successfully report back to boards.

15:00-15:30—Session Block

Combating Deliberate & Destructive Attacks: Lessons Learned from a Real Event, Unprecedented in the World History of Broadcasting

Presenter: Alexis Renard, Deputy CIO, TV5Monde

Last year, French television network, TV5Monde, was forced to broadcast only pre-recorded programs after an unprecedented hack by self-proclaimed Islamic State militants, who also hijacked its websites and social networks. After months of work spent by their incident responders to recover and reclaim their systems, much was learned. One good thing that came out of this experience was that board members at many large companies could no longer ignore what happens when hackers come knocking at their door. Nonetheless, cyber-security now tops the agenda at the TV5Monde firm. Mr. Renard will talk about the hack, lessons learned, and the new protective posture being taken to ensure no surprises come their way again.

15:30-16:00—Refreshment Break

16:00-17:00—Session Block

Cyber Security and the General Data Protection Regulation – Obligations, Challenges and Solutions

Moderator: Gershon Janssen, Chairman of the Board, OASIS

Presenters:

Wim Nauwelaerts, Partner, Hunton & Williams

Ann Cavoukian, Executive Director of the Privacy and Big Data Institute, Ryerson University (via video)

Stewart Room, Partner, Global Head of Cyber Security and Data Protection, PwC Legal

The European Commission’s 2012 EU General Data Protection Regulation (GDPR) reached political agreement by the European Parliament and the Council in December 2015 following final negotiations among the three institutions. It is expected that the GDPR will be formally adopted by the European Parliament and Council in Spring 2016, and come into force in 2018.The GDPR includes provisions that will have significant impact on businesses and governments internationally, and bring new obligations and challenges for cybersecurity policy development and operational practices. This panel will provide an overview of the regulation, focusing on key provisions that must be addressed by companies as they implement their cybersecurity programs. It will address new provisions, such as Data Protection by Design, the “Right to be Forgotten,” and increased compliance, accountability and data breach notification obligations. It will also examine analytic and methodological tools that can assist practitioners in understanding and managing their data protection risks as they design and operate cybersecurity programs.

Panel topics to include:

- GDPR Overview and Key Provisions
- Linkages: GDPR and Cybersecurity
- Data Protection by Design
- And Tools Supporting Implementation of the Regulation

17:00-17:15—Closing Remarks

Conference Chair: Freddy Dezeure, Head of CERT-EU