

Global Standards Unification

*How EU NIS Platform, NIST and IETF Standards are
Breaking Barriers for Information Sharing and
Automated Action*

27th FIRST Meeting – Berlin, June 2015

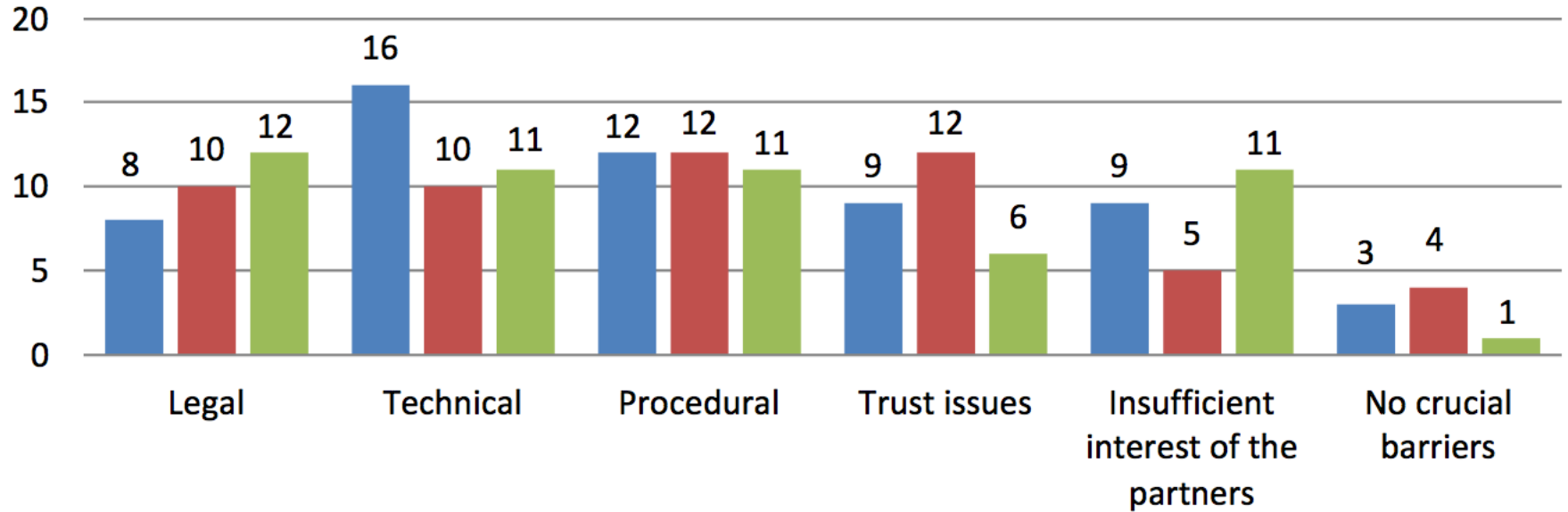
Merike Kaeo

merike@doubleshotsecurity.com

Agenda

- ◆ Existing Barriers to Information Sharing
- ◆ EU-NIS Platform / NIST
- ◆ IETF Work
- ◆ Other Related Work
- ◆ Further Improvements Needed

Barriers To Sharing: ENISA Report



- Other CERTs in the same country
- CERTs of the same type/constituency
- Operator/ISPs or Industry

Source: ENISA Detect, SHARE, Protect Report

Where Cohesiveness Needed

Technical

Creating the resilient infrastructure for data sharing that can support a variety of data types and formats.

Policy

Creating the appropriate legal structure(s) to foster comprehensive data sharing without cumbersome legal liabilities.

Governance

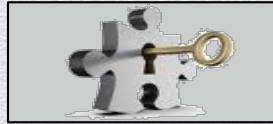
Business rules by which members of a network share, what they share, and with whom they share.

Collaboration Across Varying Boundaries

EU-NIS



NIST



IETF



European Union Network and Information Security Platform (EU-NIS Platform)

- ◆ First Meeting Held June 2013
- ◆ EU-NIS Public-Private Platform Objective
 - ◆ Consistent implementation of the NIS Directive
 - ◆ <https://resilience.enisa.europa.eu/nis-platform>
- ◆ Three Working Groups Defined
 - ◆ WG1: Risk management
 - ◆ WG2: Information exchange and incident coordination
 - ◆ WG3: Secure ICT research and innovation

EU-NIS Platform WG2 Scope

- ◆ Investigate the feasibility and needs to address the ability for an organization to share cyber threat information and to utilize a standard incident management process
 - ◆ Include current observed practices on information sharing and incident notification within EU and internationally
- ◆ Cover both public and private organizations, and all industry verticals within the private sector
- ◆ Develop SME/SMB capability in cyber security and how these sectors can benefit from the NIS platform without being overly burdened by mandatory requirements

EU-NIS Platform WG2 Discussions

- ◆ Multi-national and multi-vendor participation
- ◆ Varied discussions on trust and barriers
 - ◆ TRUST: earned via time or via contractual liability
 - ◆ Barriers: technology, trust, legal and policy
- ◆ Detailed varying sharing initiatives that are working in different countries
- ◆ Exchanged information on regulatory and privacy/liability concerns

Time to Compare EU Work With US NIST



US National Institute of Standards and Technology (NIST)

- ◆ Cybersecurity Framework
 - ◆ First version released Feb 12, 2014
 - ◆ Created thru collaboration between industry and government
- ◆ Guide to Cyber Threat Information Sharing
 - ◆ Special Publication 800-150
 - ◆ Initial draft public comment period Oct 29, 2014 – Nov 28, 2014
 - ◆ New draft based on those comments coming soon

Cybersecurity Framework Basics

- ◆ Common language for international cooperation on critical infrastructure cybersecurity
 - ◆ NOT industry specific
 - ◆ NOT country specific
- ◆ Concise way to align business risk conversations and technical operational processes

Framework Core Functions and Categories

Functions

Categories

IDENTIFY	Asset classification and management; risk assessment
PROTECT	Proactive protection and security awareness training
DETECT	Continuous monitoring and investigating anomalies
RESPOND	Response planning and mitigation
RECOVER	Post mortem and recovery planning and improvements

Framework Tiers & Profiles

- ◆ Tiers provide context on cybersecurity risk and the processes in place to manage the risk
- ◆ Profiles aligning standards, guidelines and practices
 - ◆ Create existing profile
 - ◆ Perform risk analysis of current situation
 - ◆ Create a target profile
 - ◆ Determine, analyze and prioritize gaps
 - ◆ Come up with an action plan
- ◆ Tiers do not represent maturity levels – it's more of a business risk tolerance level

Framework Added Benefits

- ◆ A reference section aligns the NIST reference categories to other compliance mandates
 - ◆ ISO
 - ◆ COBIT
 - ◆ NIST
- ◆ Many companies have started to base their security risk profiles on the NIST Cybersecurity Framework
 - ◆ Intel, Boeing, FAA, etc.
 - ◆ Smaller companies and supply chains are getting help via trainings

NIST And Special Publications

- ◆ SP 800 series are of general interest to the computer security community
- ◆ Collaborative activities with industry, government, and academic organizations

SP 800-163

Jan. 2015

Vetting the Security of Mobile Applications


 [SP 800-163](#) [FAQ](#)

doi:10.6028/NIST.SP.800-163 [\[Direct Link\]](#)

SP 800-153

Feb 2012


Guidelines for Securing Wireless Local Area Networks (WLANs)

 [SP 800-153](#)

SP 800-152
(Draft)

Dec. 18,
2014


DRAFT A Profile for U. S. Federal Cryptographic Key Management Systems (CKMS) (Third Draft)

 [Announcement and Draft Publication](#)


SP 800-150
(Draft)

Oct. 28, 2014

DRAFT Guide to Cyber Threat Information Sharing

 [Announcement and Draft Publication](#)

Guide to Attribute Based Access Control (ABAC) Definition and Considerations

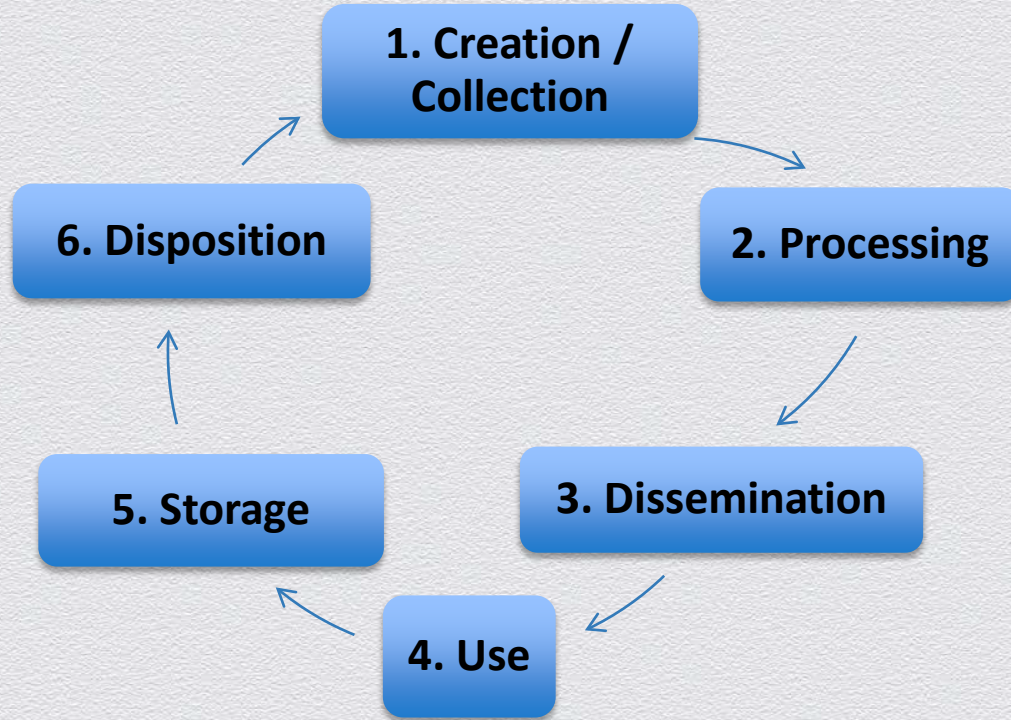
 [SP 800-162](#) [FAQ](#)

doi:10.6028/NIST.SP.800-162 [\[Direct Link\]](#)

Guide To Cyber Threat Intelligence Sharing (SP800-150) – it's a draft

- ◆ Comprehensive Document
- ◆ Covers Following Topics
 - ◆ Incident Coordination and Information Sharing Overview
 - ◆ Understanding Current Cybersecurity Capabilities
 - ◆ Establishing, Maintaining, and Using Information Sharing Relationships
 - ◆ Incident Coordination Scenarios

Managing Information Lifecycle



1. Generating or acquiring information
2. Aggregating, transforming, correlating, and classifying information
3. Publishing and distributing information to authorized recipients
4. Applying information to support organizational decision making
5. Short and long-term retention of information
6. Implementing and enforcing policies for the retention and disposal of information

What Merike Found Interesting

- ◆ EU NIS Platform work complemented the NIST work on many levels
 - ◆ Discussions on barriers to sharing, how to foster trust, what standards and formats were mostly in use, etc
- ◆ Was there any collaboration happening between the EU and US?
 - ◆ Specifically the public-private partnership discussions around information sharing challenges

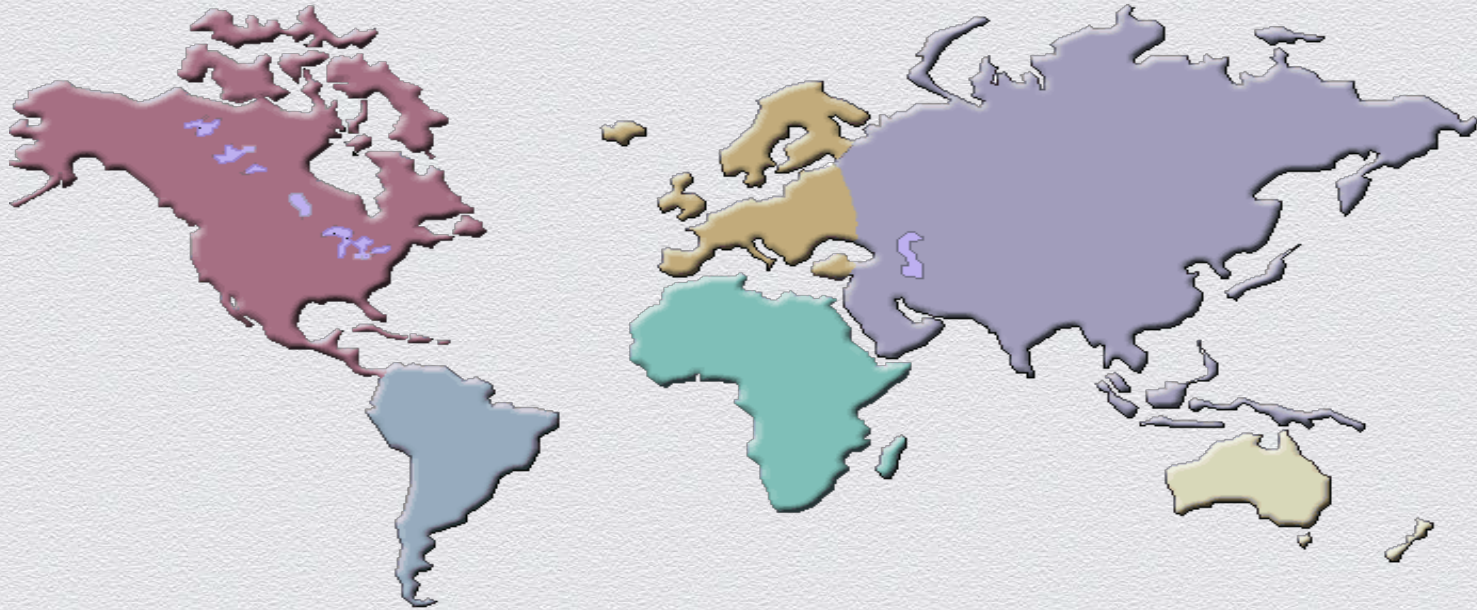
Collaboration Between US and EU

- ◆ Preliminary workshop comparing US Cybersecurity Framework and EU NIS Platform approaches in Brussels November 24, 2014
- ◆ Panel 1: Risk management practices for industry
 - ◆ Explored to what extent approaches converge and to what extent it is possible to align the initiatives moving forward
- ◆ Panel 2: Fostering voluntary sharing internationally
 - ◆ Role that voluntary information sharing mechanisms play in the US and EU
 - ◆ To what extent they are used in prevention (e.g. sharing of information on emerging threats)
 - ◆ To what extent they are used for reaction (e.g. to remedy vulnerabilities or incidents)

Takeaways from Collaboration Meeting

- ◆ No one size fits all
- ◆ Need to create an enabling environment
 - ◆ Align compliance requirements
 - ◆ Take into account country- and sector-specific needs
- ◆ Multi-Stakeholder is necessary
- ◆ Must work with SMB to help them start with basic sharing and then build up from there (also true for some less sophisticated EU member states)
- ◆ Need to define role of CEOs and Board of Directors and their respective responsibilities

What About Other Geographic Regions?



There are dialogues happening with multiple different geographic regions

Internet Engineering Task Force (IETF)

- ◆ Mission: Make the Internet better from an engineering point of view
- ◆ Early work on security practices and incident response
 - ◆ RFC 2196: Site Security Handbook (September 1997)
 - ◆ RFC 2350: Expectations for Computer Security Incident Response (June 1998)
 - ◆ RFC 3013: Recommended Internet Service Provider Security Services and Procedures (November 2000)
 - ◆ RFC 3227: Guidelines for Evidence Collection and Archiving (February 2002)

IETF – Foundational Completed Work

Working Group	Comments
IPFIX (IP Flow Information Export)	<ul style="list-style-type: none">- Specified the information model (to describe IP flows)- Specifies the IPFIX protocol (to transfer IP flow data from IPFIX exporters to collectors)
INCH* (Incident Handling)	<ul style="list-style-type: none">- Defined a framework (IODEF) to represent computer and network incidents- Defined a protocol (RID) to facilitate sharing computer and network security incidents.
SYSLOG (Security Issues in Network Event Logging)	<ul style="list-style-type: none">- Standardized the protocol to log events- Standardized the secure and non-secure transports of the syslog protocol
NEA (Network Endpoint Assessment)	<ul style="list-style-type: none">- Defined a mechanism to evaluate the posture of a system

IETF – Work in Progress

Working Group	Comments
MILE (Managed Incident Lightweight Exchange)	<ul style="list-style-type: none">- Ongoing work to revise IODEF documents to incorporate enhancements and extensions based on operator experience- Provide guidance on RID transports.- Define a resource-oriented approach to cyber security information sharing that follows the REST architecture [ROLIE].
SACM (Secure Automation and Continuous Monitoring)	<ul style="list-style-type: none">- Enhances the work done in NEA to define a set of standards to enable assessment of endpoint posture- Create a set of standards for interacting with repositories of content related to assessment of endpoint posture

IETF – New Working Groups

Working Group	Comments
I2NSF (Interface To Network Security Function)	<ul style="list-style-type: none">- Will define an information model, a set of software interfaces and data models for controlling and monitoring aspects of physical and virtual Network Security Functions.- Focus will be on functions that provide treatment to packets/flows, such as IPS/IDS, Web filtering, flow filtering, deep packet inspection, or pattern matching and remediation- Goal is to enable enterprises to utilize security functions not hosted on their own premise but instead hosted in service provider domain and to establish how to communicate desired security policies to NSF

IETF – New Working Groups

Working Group	Comments
DOTS (DDoS Open Threats Signaling)	<ul style="list-style-type: none">- Develop a standards based approach for the realtime signaling of DDoS related telemetry and threat handling requests- Concerned with DDoS attack detection, classification, traceback, and mitigation- Resulting standards will be designed so they apply to network security applications beyond the DDoS problem space- Specifications will include a standard mechanism for authentication and authorization, data integrity, and providing for privacy in operation, with privacy-friendly choices being the default in all cases

Let's Not Forget Law Enforcement

A shared due process framework is needed to enable interoperability between heterogeneous stakeholders and normative orders in order to prevent a fragmentation of cyberspaces along national border



Internet and Jurisdiction Project
<http://www.internetjurisdiction.net>

Internet and Jurisdiction Basics

Areas of Cooperation

- ◆ Domain Seizure
- ◆ Content Takedown
- ◆ Access to Subscriber Data

Read latest report:

<http://www.internetjurisdiction.net/wp-content/uploads/2015/01/Internet-Jurisdiction-Project-Progress-Report-2013-14.pdf>

Building Blocks

- ◆ **Authentication:** verify identity and authority
- ◆ **Transmission:** standard submission formats and routing mechanisms
- ◆ **Traceability:** transparency reports; logging
- ◆ **Determination:** criteria for compliance with requests and role of neutral 3rd party
- ◆ **Safeguards:** user notification, right of response and appeal mechanism
- ◆ **Execution:** implementation modalities to avoid unintended consequences

What's In Our Future?

- ◆ We have many comprehensive guidelines
- ◆ There are many cross functional dialogues happening
- ◆ We have many data sharing formats that are standardized (or in process of getting standardized)
- ◆ We do NOT have simplicity
- ◆ Next steps:
 - ◆ Continue collaborating across geographic areas and operational, technical, political, legal, policy sectors
 - ◆ Start sharing something with someone and lets work policy, process and technical issues in parallel