RSACONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

Collaboration Across The Threat Intelligence Landscape

SESSION ID: ANF-F02

Merike Kaeo

CISO, IID
merike@internetidentity.com

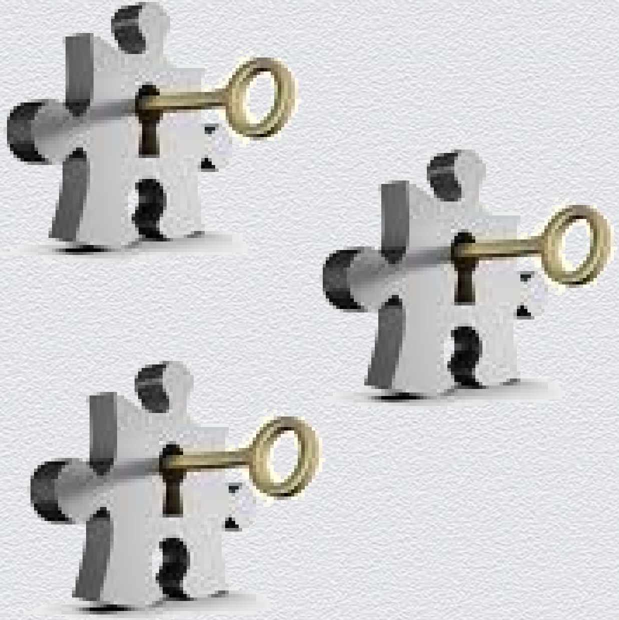
Topics For Today

- Introduction and Background
- Ongoing Sharing Efforts
- Existing Standards And Frameworks
- Global Efforts To bring About Action
- Where Do We Go From Here?

Introduction and Background

What’s So Important About Sharing?

- Everyone knows sharing is fundamentally good
- Many discussions around wanting to share
- Government, private sector and public sector alliance efforts have been ongoing
- More action is needed



The Criminals Are Really Good At Sharing

- Websites advertise Botnets and Malware for hire
- Vulnerabilities and Exploits are traded on an ‘open market’
- There are no enforceable rules for NOT sharing
- Utilizing social media is making sharing much more efficient

Choose Custom Botnet

- Number of Hosts
- Geographic Region
- Bandwidth
- Duration
- etc

Areas In Need of Improvement

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.

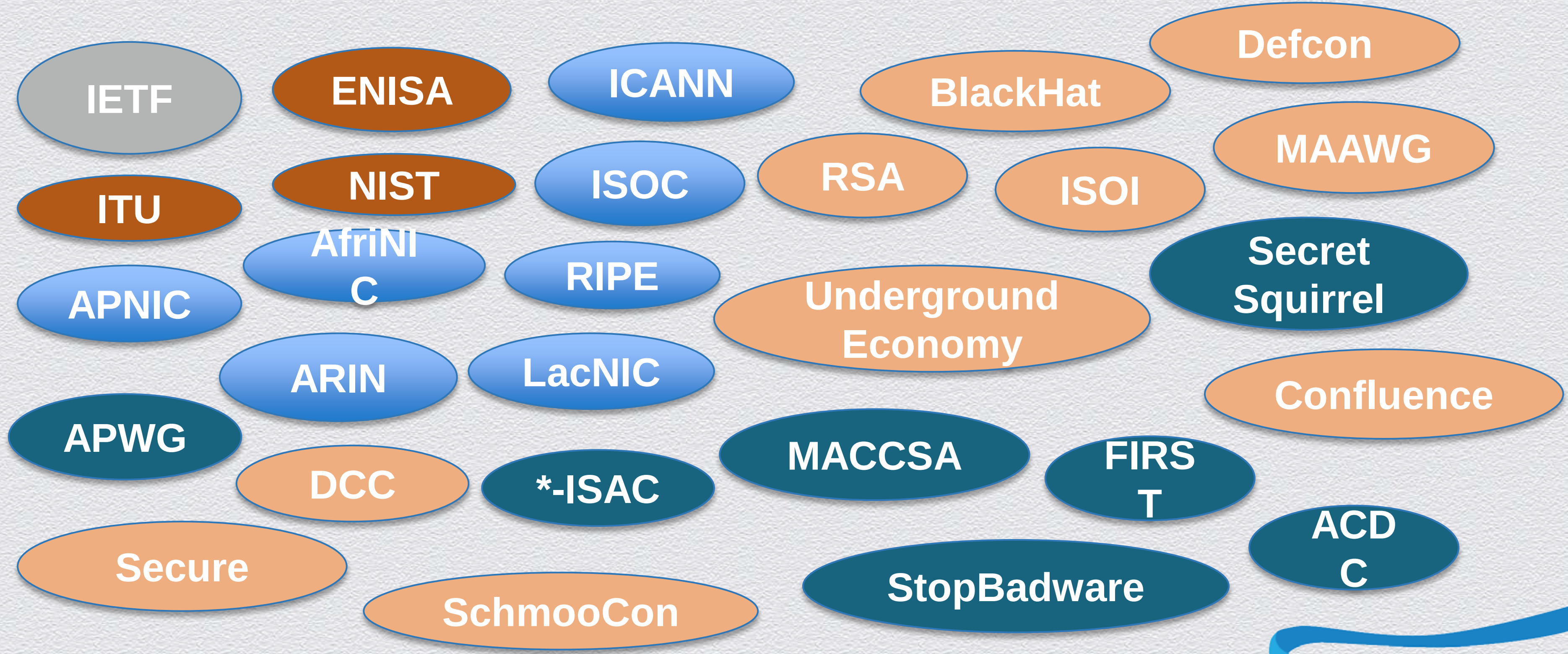
Governance

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

→ **We Need A Paradigm Shift!**

Ongoing Sharing Efforts

Sharing Landscape – Who Is Doing What



IETF

ITU

APNIC

APWG

Secure

ENISA

NIST

AfriNI
C

ARIN

DCC

ICANN

ISOC

RIPE

LacNIC

*-ISAC

SchmooCon

BlackHat

RSA

Underground
Economy

MACCSA

StopBadware

Defcon

MAAWG

ISOI

Secret
Squirrel

Confluence

FIRS
T

ACD
C

Sharing Landscape – Wait There's More…..

Industry Sectors

Aerospace, Aviation, Chemical Industry, Construction, Consumer Products, Education, Energy, Environment, Financial (Banking, Exchanges, Insurance, Payments), Food, Health, Heating&Ventilation, Machine Safety, Materials, Nanotechnology, Oil&Gas, Pharmaceutical, Research Facilities, Services, Smart Metering, Space, Transport (Road, Rail, Shipping), etc.

National Initiatives

UN, NATO, EU, Africa, Asia, National CERTs, etc.

Data Sharing Groups

Who Defines Membership?

- Some are open to all
- Some are personality driven
- Some are interest driven
- Some are highly peer vetted
- Some are geographically focused

Trust Levels

- Is trust transitive?
- How is trust lost?
- Can trust be regained?
- How do you define varying degrees of trust?

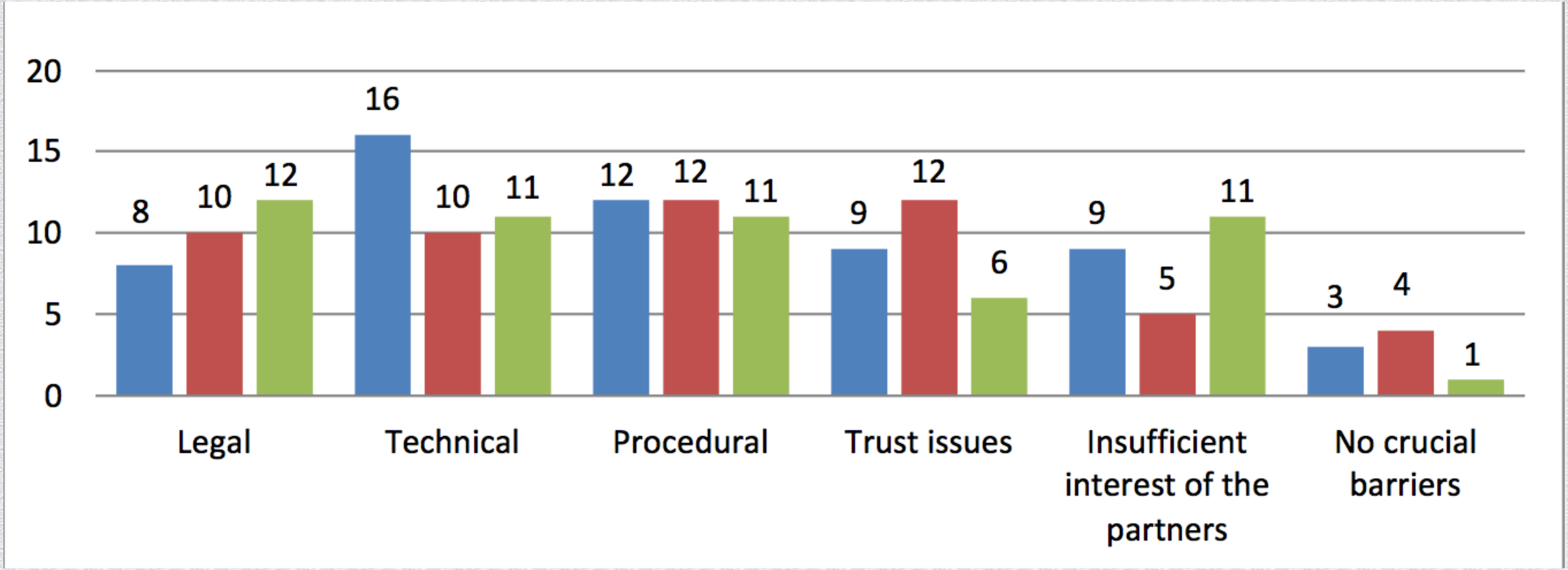
Examples of Specializations

- FIRST: Vulnerability Management
- MAAWG / APWG: Anti SPAM, Phishing and Crime
- DNS-OARC: DNS System Security
- NSP-SEC: Big Backbone Providers and IP Based Remediation
- ISACS: Specialized Interest Groups
- OPSEC-Trust: Situational Awareness

We Must Learn What Sharing Actually Means

- Sharing is NOT “You give me all your information and I will use it”
- Sharing is NOT “I will not contribute to any of the information”
- Sharing is NOT “I will secretly give this information to people”
- Sharing is NOT “We need another secret group to learn to share”
- Sharing IS “Let’s work together to bridge the existing silos”
- Sharing IS “Collaboration and creating governance structures to limit sharing where legally necessary”

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

Ultimate Goal

- Actionable Intelligence
- Better intelligence translates to better protection
- Increased protection translates to less fraud and decrease in revenue loss
- Collective intelligence is far more effective than individual silos

Existing Standards And Frameworks

How Do People Share Today?

Format	Comments
Email	Very common but inefficient
CSV	No complex detail is included
PDF	Very common but inefficient
XML	Used for events (txt) or network traffic (pcap) Human readable and machine parsable but is verbose and introduces information bloat
JSON	Text based and human-readable

MITRE/NIST Specifications - Enumerations

Specification	Description
CAPEC: Common Attack Pattern Enumeration and Classification	List of common attack patterns - includes comprehensive schema and classification taxonomy
CCE: Common Configuration Enumeration	Nomenclature and dictionary of system configuration issues
CEE: Common Event Expression	Nomenclature to describe, encode and exchange event log and audit data (no funding as of mid 2013)
CPE: Common Platform Enumeration	Nomenclature and dictionary of product names and versions
CVE: Common Vulnerability and Exposures	Nomenclature and dictionary of security-related software flaws
CWE: Common Weakness Enumeration	Formal list of common software weaknesses
MAEC: Malware Attribute Enumeration and Characterization	Standardized language for encoding malware information

MITRE/NIST Specifications – Vulnerability Measurement/Scoring

Specification	Description
CVSS: Common Vulnerability Scoring System*	Vulnerability scoring system for rating IT vulnerabilities
CCSS: Common Configuration Scoring System	Set of measures of severity of software security configuration issues (derived from CVSS)
CWSS: Common Weakness Scoring System	Framework for prioritizing security errors that are discovered in software applications (conceptually similar to CVSS)

* Created and Maintained by FIRST

MITRE/NIST Specifications – Expression, Checking and Reporting Languages

Specification	Description
CVRF: Common Vulnerability Reporting Format	Enables software vulnerability information to be shared in machine-parsable format (XML based)
OCIL: Open Checklist Interactive Language	Language for expressing and evaluating manual security checks
OVAL: Open Vulnerability and Assessment Language	Language for specifying low-level testing procedures used by checklists
XCCDF: Extensible Configuration Checklist Description Format	Language for specifying checklists and reporting checklist results

IETF Standards That Are Relevant to Sharing

Working Group	Description of Work Created or In Progress
INCH: Extended Incident Handling	- IODEF which defines an information model for security incidents - RID is a protocol for exchange of information and utilizes TLS
MILE: Managed Incident Lightweight Exchange	- Working on extensions to IODEF to specify how it can be integrated into other standards
MARF: Messaging Abuse Reporting Format	- ARF (Abuse Reporting Format) that is MIME based - Carried within SMTP envelopes and was extended to support DKIM and SPF authentication failure reports
NEA: Network Endpoint Assessment	- Assess endpoints and determine compliance with security policies - PA-TNC (Posture Attribute Protocol)/PB-TNC (Posture Broker Protocol)
SACM: Security Automation and Continuous Monitoring	- Aims to define protocol and data format standards that enable retrieval and collection of endpoint posture information

NIST: Security Content Automation Protocol (SCAP)

- Version 2 Technical Specification
  - http://csrc.nist.gov/publications/nistpubs/800-126-rev2/SP800-126r2.pdf
- Components include
  - ARF – Asset Reporting Format
  - CCSS – Asset Identification, Common Configuration Scoring System
  - TMSAD – Trust Model for Security Automation Data
  - OVAL – Open Vulnerability Assessment Language
  - CPE – Common Platform Enumeration
  - XCCDF – Extensible Configuration Checklist Description Format

Sharing Needs and Realities

- Two primary needs
  - Machine-parsable large data sets
  - Human-readable data sets
- Automation means structured data
- Realities of today – structured data still evolving
  - People define new object types to fix some of the problems and then write scripts (“tools”) to let people send information
  - Many varying types of structured data

‘Standards’ - We Are NOT Done Yet……

Taxonomies/Frameworks

- IODEF – Information Operations Description Exchange Format
- CIF – Collective Intelligence Framework
- STIX – Structured Threat Information Expression
- OpenIOC – Open Indicators of Compromise
- Veris – Vocabulary for Event Recording and Incident Sharing

Transports

- RID – Real-time Inter-network Defense
- TAXII – Trusted Automated Exchange of Indicator Information
- XMPP – Extensible Messaging and Presence Protocol
- NMSG – Network Message (also a structured frame format)
- SOAP – Simple Object Access Protocol

IODEF

- Provides a data model to accommodate most commonly exchanged data elements and associated context for indicators and incidents
  - http://www.ietf.org/id/draft-ietf-mile-rfc5070-bis-06.txt
- IODEF-Extensions For Structured Cybersecurity Infromation
  - http://www.ietf.org/id/draft-ietf-mile-sci-13.pdf
  - Extension Classes: *Attack Pattern, Platform, Vulnerability Scoring, Weakness, Event Report, Verification, Remediation*
  - Standards: *CAPEC, CEE, CPE, CVE, CVRF, CVSS, CWE, CWSS, OCIL, OVAL, XCCDF*

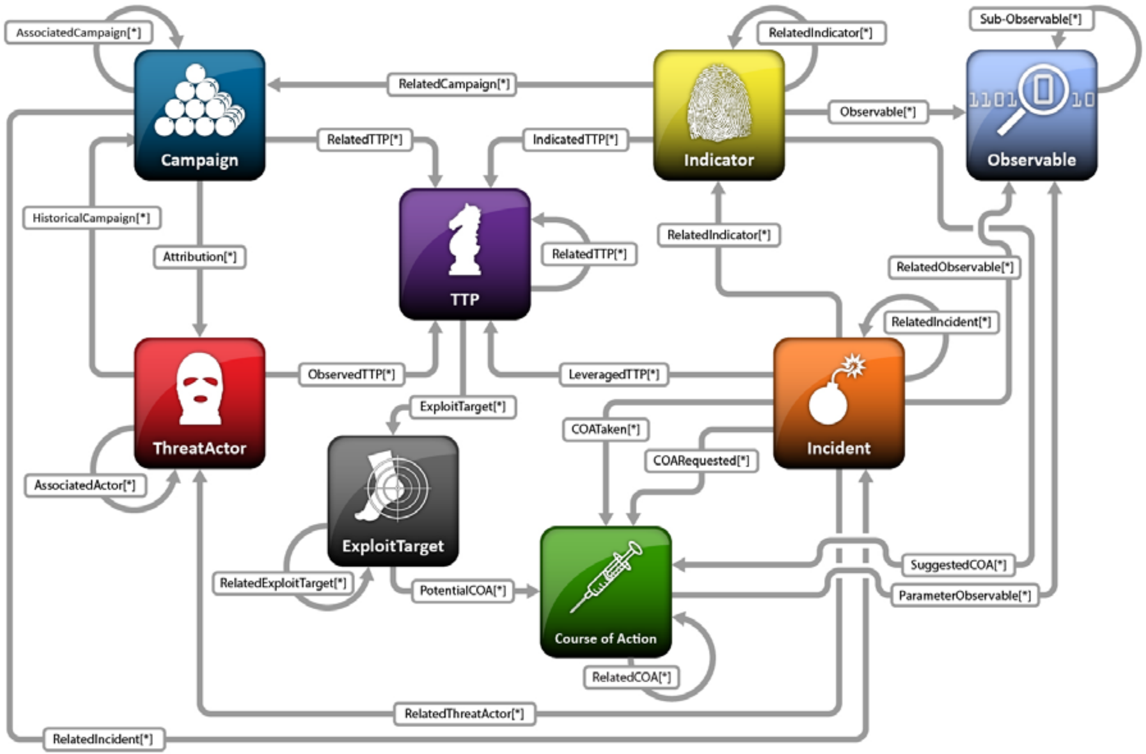
CIF

- A cyber threat intelligence management system.
  - Can combine known malicious threat information from many sources
  - Use that information for action: identification (incident response), detection (IDS) and mitigation (null route)
- Keep it simple and don't overthink it
- It's all about the tools!
  - csirtgadgets.org/examples
  - csirtgadgets.org/preso

STIX

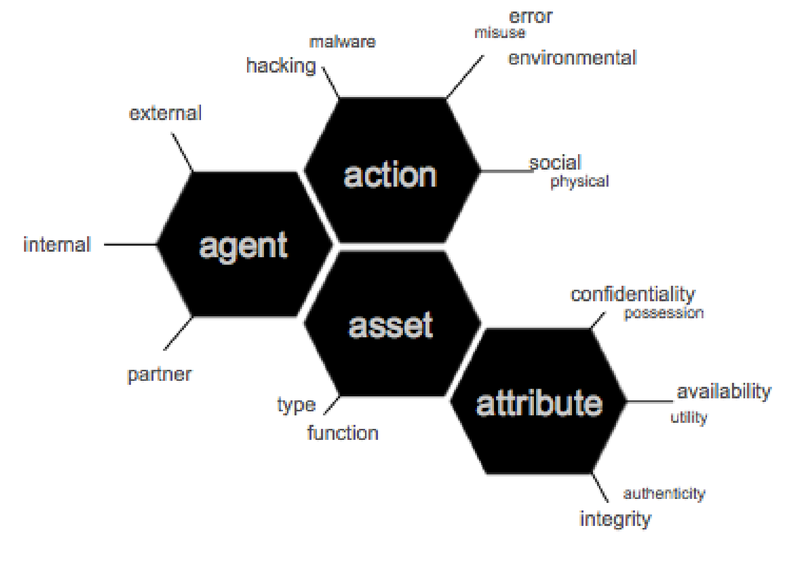
- Provides common mechanism for addressing structured cyber threat information across wide range of use cases
  - Analyzing Cyber Threats
  - Specifying Indicator Patterns for Cyber Threats
  - Managing Cyber Threat Response Activities
    - Cyber Threat Prevention
    - Cyber Threat Detection
    - Incident Response
  - Sharing Cyber Threat Information

Structured Threat Information eXpression (STIX) v1.1 Architecture



VERIS

- VERIS is a (open and free) set of metrics designed to provide a common language for describing security incidents (or threats) in a structured and repeatable manner.
- DBIR participants use the VERIS framework to collect and share data.
- Enables case data to be shared anonymously to RISK Team for analysis
- More at http://veriscommunity.net/



Actor – Who?

Action – How?

Asset – What?

Attribute – Outcome?

OpenIOC

- An XML-based standardized format for sharing Threat Indicators
- Open Source as Apache2 since 2011
- Derived from years of “What Works” for Mandiant
  - Indicator Terms
    - Artifacts on Hosts and Networks
  - Logical Comparisons
    - Groupings, Conditions
  - Ability to Store & Communicate Context
  - Continues to be developed and improved upon (http://openioc.org)

NMSG

- NMSG is a file and wire format for storing and transmitting user-defined blobs of information
  - User-defined blobs of information on the order of 10 - 10,000 octets long
  - Network transport optimized for jumbo frame UDP broadcast on a LAN
  - Framing encoded using Google Protocol Buffers
    - Ideal for data that needs binary clean encoding (network packets/DNS messages)
- https://github.com/farsightsec/nmsg

Thoughts on Schemas / Frameworks

- Use existing ones to start sharing SOMETHING
- Start sharing data utilizing what you have available
    - Syslog data is a good start
    - PDF or CSV formatted data from security devices is a good start
- Only by starting to share in an automated way will gaps in schemas get identified (and FIXED)
- Let's not forget the tools!

Don’t Always Need Everything - Look At Use Cases

- Specific data needs for Takedowns
- Specific data needs for Law Enforcement
- Specific data needs for Network Mitigation
- Specific data needs Vulnerability Disclosure
- Specific data needs for International Cooperation
- etc

We Need To Figure Out Minimum Details To Share For Some Specific Types Of Use Cases !

RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Global Efforts to Bring About Action

Georgetown University S2ERC

- Security and Software Engineering Research Center
  - Cyber Threat Intelligence Sharing Ecosystem Program
    - http://s2erc.georgetown.edu/projects/cyberISE/
    - Contact: Eric Burger [eburger@cs.georgetown.edu]
  - Participation
    - Enterprises and end users
    - Organizations responsible for operating secure networks and systems
    - Vendors of cybersecurity products and services
    - Information-sharing organizations that produce, vet, collect, analyse and distribute cyber threat intelligence on behalf of stakeholders

EU Network and Information Security (NIS)

- NIS Public-Private Platform Objective
  - Consistent implementation of the NIS Directive
    - WG1: Risk management
    - WG2: Information exchange and incident coordination
    - WG3: Secure ICT research and innovation
- Specifics to WG2
  - Multi-national and multi-vendor participation (IID is contributing)
  - https://resilience.enisa.europa.eu/nis-platform/shared-documents/wg2-documents/wg2-outcome-draft/view

Global Sharing Initiatives – Some Comments

- ACDC
- APWG eCRIME
- ISACs [10 but which are actively sharing?]
- NATO CDXI
- CERT initiatives [there are many]
- MACCSA
- CIRCAS

Privacy Aspects – A Global Perspective

- Terminology
  - Data Protection Law / Privacy Law / Data Privacy Law
- Many global initiatives that are continually progressing
  - European Union - Data Privacy Legislation Update
  - Africa – Leading Initiative from Economic Community of West African States
  - Asian and Oceania
  - The Americas
- A good read and hot off the press:
  - Data Privacy Law, An International Perspective by Lee A. Bygrave

Where Do We Go From Here?

Start Sharing What You Can

- Start by sharing for specific use cases that don’t impact privacy/PII
  - SSH Brute Force Attack
  - DNS/SNMP/NTP Amplification Attack
  - Passive DNS Information
- Investigate how to share data that may impact privacy/PII and what can be anonymised but still be useful
  - SPAM / Phishing details
  - Content could raise PII issues but where?

We Need To Break These Barriers NOW

- Ownership
  - It should become possible to fuse proprietary and non-proprietary information, particularly threat intelligence information, whilst protecting the commercial interests of proprietary information providers.
- Liability
  - A liability model(s) should be available to protect the interests of all parties in a way that is balanced with achieving community benefit from sharing information

Practical Considerations

- Performance Aspects
  - Parsing Speed
  - Storage Size
  - Bandwidth
  - Memory
- How do I fix errors and conflicts QUICKLY
  - False Positives
  - Discrepancies
  - Governance Violators

Parting Thoughts

- Are you willing to share data?
- What information do you want to share?
- How do you justify sharing the information?
- Do you know with whom to share data with?
- How do you comply with (international) law?
- How will you interconnect with other silos that you are a part of?
- What are YOUR impediments to data sharing across silos?

QUESTIONS?