Practical Intelligence Sharing: ISACs and ISAOs: Welcome!

Laura Koetzle
Vice President and Group Director
Forrester
@lkoetzle
2014 Submission Titles

- Cyber
- Network
- Risk
- Attacks
- Mobile
- Data
- Cloud
- Threat
2015 Submission Titles
Yep, still a problem in 2017 (and plural!)
Our agenda for today

- Now-9:50: Cyber Information Sharing: Are We Still Talking About This? A 360 POV
- 9:55-10:35: A Tale of Four ISACs
- 10:40-11:20: Ad hoc Threat Intelligence: Two Unlikely Partners Combine to Enhance Intel
- 11:25-12:05: Closing the Gap Between Public and Private Threat Intelligence Sharing
When you leave this room, you’ll have:

- Practical techniques for getting more out of the intelligence sharing processes and bodies you participate in now
- New ways to use existing toolsets to enhance intelligence capture and sharing
- New connections for intelligence sharing beyond your industry, region, or area of expertise
So let’s get going!

Laura Koetzle
+31 (0)20 305 4345
lkoetzle@forrester.com
@lkoetzle
<table>
<thead>
<tr>
<th>Start Time</th>
<th>Title</th>
<th>Presenters</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:10 AM</td>
<td>Cyber Information Sharing: Are We Still Talking About This? A 360 POV</td>
<td>Bobbie Stempfley, Bruce Bakis, Faye Francy, Carole Rendon, John B. Wood</td>
</tr>
<tr>
<td>9:55 AM</td>
<td>A Tale of Four ISACs</td>
<td>Marcus Sachs, Michael Arceneaux, John Carlson, Joseph Viens</td>
</tr>
<tr>
<td>10:40 AM</td>
<td>Ad Hoc Threat Intelligence: Two Unlikely Partners Combine to Enhance Intel</td>
<td>Chris Matthieu, John Smith</td>
</tr>
<tr>
<td>11:25 AM</td>
<td>Closing the Gap Between Public and Private Threat Intelligence Sharing</td>
<td>Jason Smith, Sean Duca</td>
</tr>
</tbody>
</table>
Cyber Information Sharing: Are we still talking about this? A 360° POV

Bruce Bakis
Manager, Cyber Sharing Partnerships
The MITRE Corporation @bjbakis

Faye Francy
Executive Director
Automotive-ISAC

Carole Rendon
U.S. Attorney, Northern District of Ohio
Department of Justice

Bobbie Stempfley
Director, Cyber Implementation
The MITRE Corporation @bobbiestempfley

John B. Wood
CEO and Chairman of the Board
Telos
Key Discussion Points

ISAC Operator: risk ↓
member ROI ↑

Member: value?

ISAO: catalyze?

Government & Law Enforcement: ?

• why join...which one?
• State and local Governments?
• how NOT to make a bad one?
• what is good?
• ROI/value?
• The government & law enforcement good/bad?

is space too crowded?
metrics?
federation?
scale trust?

MITRE
Contact Information

- Bobbie Stempfley, rgs@mitre.org
- Bruce Bakis, bbakis@mitre.org
- Faye Francy, fayefrancy@automotiveisac.com
- Carole Rendon, carole.rendon@usdoj.gov
- John Wood, john.wood@telos.com
Address the Gnarly 9

Mission

Value

Ecosystem

Milestone

Membership

Leadership

Information

Trust

Funding
Auto-ISAC

Faye Francy
Auto-ISAC Value Proposition

Protecting the Automotive Sector

‘To reduce the risks and costs associated with disruption to automotive industry due to cybersecurity events’

Needs
- Mitigation of business risks
- Maintaining public trust

Offering
- Comprehensive, across the connected vehicle
- Preparedness, response, and recovery planning
- Strategic coordination with partners

What we don’t do
- Law enforcement activities
- Security infrastructure design
- Policy

Benefits
- Timely & actionable threat information
- Common view of cyber threat intelligence
- Fusion and analysis of threat-based info
- Protection of private sector data
- Sharing of best security practices
Trusted Information Sharing and Analysis
Cyber Threat and Vulnerability Intelligence

Central Hub for Intelligence and Analysis

Manufacturers

US Govt Cyber Feeds

Best Practice Identified

Incident Occurred

Remediation Complete

Vulnerability Detected

Vendor Threat Feed

Supplier

Benefits

 Efficiently identify threats by supplementing internal intelligence with external feeds

Detect vulnerabilities faster with cross-industry vulnerability information sharing

Validate risk analysis with reliable industry-level findings and best practices

Aggregate, analyze and share auto-specific cyber information across the industry’s attack surface
Best Practice Development

Our Objectives
1. Define best practices for securing the connected vehicle ecosystem
2. Provide guidance on how to implement best practices

Our Phased Approach

1. Define Scope & Identify Core Team
2. Build Reference Model
3. Develop Executive Summary & One Best Practice Guide
4. Socialize with Stakeholders
5. Create Communications Strategy & Continuously Improve
The Automotive Community Working Together

- **28 OEMs**
- **16 OEMs & 12 suppliers from 3 continents actively participating in best practices working sessions**, along with the Auto Alliance and Global Automakers.

- **65+ SMEs**
- **65 Auto-ISAC member company SMEs with expertise in design, engineering, safety, legal, public policy, and other disciplines.**

- **1000+ hours**
- **75+ hours of small and large group working sessions**, amounting to over 800 man-hours towards development since February.

- **300+ BPs**
- **Documented mapping of best practices to over 35 industry standards and references.**

- **300+ BPs**
- **Over 300 Best Practice Statements developed to-date.**
Testifying for the first time since becoming FBI director in September, James Comey told the Senate homeland security and government affairs committee that cyber-attacks were likely to eclipse terrorism as a domestic danger over the next decade.

“That’s where the bad guys will go,” Comey said. “There are no safe neighborhoods. All of us are neighbors [online].”
IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

BOGDAN NICOLESCU,
TIBERIU DANEL, and
RADU MICLIAUS,

Defendants.

The Grand Jury charges:

General Allegations

1. Defendants BOGDAN NICOLESCU (NICOLESCU), TIBERIU DANEL (DANEL), and RADU MICLIAUS (MICLIAUS), and others presently known and unknown to the
Grand Jury (herein after referred to as the BAYROB GROUP), are members of a criminal
conspiracy located in and around Bucharest, Romania.

2. Some of the victims of the criminal schemes carried out by the BAYROB
GROUP resided in the Northern District of Ohio. Specifically, some of the computers infected
with malware by the BAYROB GROUP were in the Northern District of Ohio, some of the
computers accessed by the BAYROB GROUP without authorization were in the Northern
District of Ohio, and some of the victims who had their identities, money, or personal identifying
ISACs Were Introduced in 1998...
## Seminar Schedule

<table>
<thead>
<tr>
<th>Start Time</th>
<th>Title</th>
<th>Presenters</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:55 AM</td>
<td>A Tale of Four ISACs</td>
<td>Marcus Sachs, Michael Arceneaux, John Carlson, Joseph Viens</td>
</tr>
<tr>
<td>10:40 AM</td>
<td>Ad Hoc Threat Intelligence: Two Unlikely Partners Combine to Enhance Intel</td>
<td>Chris Matthieu, John Smith</td>
</tr>
<tr>
<td>11:25 AM</td>
<td>Closing the Gap Between Public and Private Threat Intelligence Sharing</td>
<td>Jason Smith, Sean Duca</td>
</tr>
</tbody>
</table>
A Tale of Four ISACs

**MODERATOR:** Marcus H. Sachs, P.E.
SVP and CSO, North American Electric Reliability Corporation (Electricity ISAC)
@MarcusSachs

**PANELISTS:**
- **Michael Arceneaux**
Managing Director
Water Information Sharing and Analysis Center (Water ISAC)
- **John Carlson**
Chief of Staff
Financial Services Information Sharing and Analysis Center (FS-ISAC)
@JohnCar02732441
- **Joseph R. Viens, CPP**
Sr. Director, Government Affairs
Charter Communications (Chair, Comm-ISAC)
What is an ISAC?

- Information Sharing and Analysis Centers help critical infrastructure owners and operators protect their facilities, personnel and customers from cyber and physical security threats and other hazards.
- ISACs collect, analyze and disseminate actionable threat information to their members and provide members with tools to mitigate risks and enhance resiliency.
- ISACs reach deep into their sectors, communicating critical information far and wide and maintaining sector-wide situational awareness.
ISAC Background

- Information sharing organizations have their roots in technical standards groups, government agencies, and sector roundtables.
- The concept of ISACs was introduced and promulgated pursuant to Presidential Decision Directive-63 (PDD-63), signed May 22, 1998 in the Clinton Administration.
- Some ISACs formed as early as 1999, and most have been in existence for ten to fifteen years.
- Recently a new concept – the Information Sharing and Analysis Organization (ISAO) – was introduced by the Obama administration.
Electricity ISAC

- Launched in 1999 as the ES-ISAC by the North American Electric Reliability Corporation as a voluntary information sharing group
- Became a key part of NERC’s mandatory reliability standards mission in 2006 as a collector of incident information in the bulk power system
- Was re-branded in 2015 as the E-ISAC, and segregated from NERC’s compliance and enforcement functions
- Provides both physical and cyber analysis, conducts exercises, and hosts classified and unclassified workshops, events, and briefings
- Over 4000 members in the USA, Canada, and Mexico
Water ISAC

- Launched in 2002 as a nonprofit by the national water utility industry
- Members include hundreds of utilities in the U.S., Canada, Australia and the U.K.
- Provides intelligence, analysis and guidance to reduce cyber and physical security risks
- Helps utilities improve resilience and protect public health
Financial Services ISAC

- Launched in 1999 as a non-profit designed, developed, and owned by the financial services industry
- About 7,000 financial institutions in 36 countries
- Expanding range of services:
  - Information sharing, analysis, threat monitoring & crisis escalation
  - Automation (created and sold “Soltra” which stimulated market for STIX/TAXII)
  - Support for Financial Systemic Analysis and Resilience Center (FSARC), Sheltered Harbor, regional coalitions, ISAOs, and Financial Services Sector Coordinating Council
  - Conferences/Education/Training/Exercises
  - Best Practices/Advisories
  - Crisis Communications
Communications ISAC

- Launched in 2000 when the White House designated the National Coordinating Center for Telecommunications (NCC) as the Information Sharing and Analysis Center (ISAC) for Telecommunications
- The NCC-Communications ISAC facilitates the exchange of vulnerability, threat, intrusion, and anomaly information amongst government and industry telecommunications participants
- 63 industry members/multiple government agencies
- Weekly meetings, joint exercises and activations
Apply What You Have Learned

- Next week you should:
  - Join your sector’s ISAC!
  - Or, if you are already a member – recruit a new company to join!

- In the first three months following this presentation you should:
  - Voluntarily submit at least one summary of a security event you handled

- Within six months you should:
  - Implement an automatic information sharing system (STIX/TAXII, etc.)
  - Provide feedback to your ISAC on your experience, to include suggestions for your ISAC’s improvement
More Information

- Electricity ISAC:  [www.eisac.com](http://www.eisac.com)
- Water ISAC:  [www.waterisac.org](http://www.waterisac.org)
- Financial Services ISAC:  [www.fsisac.com](http://www.fsisac.com)
- All other ISACs:  [www.nationalisacs.org](http://www.nationalisacs.org)
<table>
<thead>
<tr>
<th>Start Time</th>
<th>Title</th>
<th>Presenters</th>
</tr>
</thead>
<tbody>
<tr>
<td>10:40 AM</td>
<td>Ad Hoc Threat Intelligence: Two Unlikely Partners Combine to Enhance Intel</td>
<td>Chris Matthieu, John Smith</td>
</tr>
<tr>
<td>11:25 AM</td>
<td>Closing the Gap Between Public and Private Threat Intelligence Sharing</td>
<td>Jason Smith, Sean Duca</td>
</tr>
</tbody>
</table>
Ad Hoc Threat Intelligence

John Smith
Solutions Architect
ExtraHop Networks
@jmsazboy || @wiredata

Chris Matthieu
Director IoT
Citrix Systems
@octoblu
Traditional INFOSEC (whack-a-malware) vs. Ad Hoc Threat Intel (Trap-door spider casting net)
The Challenge

- To adapt to a changing threat landscape
- To expand use of Threat Intelligence beyond perimeter-centric and forensic (logs) approaches
- To more effectively use Open Source Threat Intelligence
- “Intel, Intel Everywhere”, and not a drop to drink (How do we make the Threat Intelligence tactile?)
One Solution: Ad Hoc Agility

- Play a baseball game
  - Hit the ball
  - Bunt the ball
- Unwanted guests (Layer 1 Resolution)
  - Not-so subtle way to ask them to leave
- Zombie Apocalypse
  - Dispatch the walking dead
The Changing Threat Landscape

- The emergence of the “Human Vector”
- Infected / vulnerable B2B partners
- Service Accounts with elevated permissions
- Weak credentials
- Working conditions in the Enterprise/Agency
  - Skeleton crews
  - Employee apathy
  - Disgruntled employees
  - Insider threats
- IoT (Internet of Things Threats)
The IoT Calamity

- Millions of devices have been rushed to market with with essentially NO security whatsoever
- They have default (some hard-coded) vendor credentials
- They will be installed and forgotten in homes and not in organizations that have a security apparatus
- The botnet(s) that will surface from them will dwarf any PC based botnet that has ever existed
- To put it simply, its **too late** to put the horse in front of the cart, you are better served preparing for the coming calamity
Shrinking Time to Compromise

- Shutter-speed of traditional security tools does not always catch new threats

**Time to Compromise**

- Detection Deficit
- The new reality
- Where Syslog/Machine Data is typically used
- Yesterday’s Threats

Verizon 2016 DBIR
Ability to Detect a Breach

Figure 9.
Breach discovery methods over time, (n=6,133).

Verizon 2016 DBIR
Why Wire Data?

- Not all systems log effectively
- The quality of logs depend on the developer of the application
- Once a system is rooted, logs are routinely shut off and/or deleted
- IoT devices (usually) don’t have any logging capability
Wire Data driven Solutions

- Bro IDS
- Wireshark/LUA API
- Corvil Networks
- Riverbed
- Netscout
- iNetCo
- ExtraHop Networks
What is Octoblu?
Malicious Surveillance Process

- ExtraHop appliance sets parameters for malicious activity at the DNS lookup phase
- ExtraHop sends a JSON payload to an Octoblu trigger with the client, server and DNS query
- Octoblu forwards the JSON payload information to the Virustotal API
- Octoblu evaluates the response from the Virustotal API adding the relevant response information then checks the response code to see if there is an acceptable score (> 70)
- Octoblu prepares the message then sends a warning email to CSIRT warning of malicious content being accessed. The email contains information on the client IP, server IP, reputation score and dossier from Virustotal.
Other API/Orchestration Driven Solutions

- Phantom (2016 innovation sandbox winner)
- CIFv2 or CIFv3 API
- Open source API solutions
  - RestifyDB
  - Ramses
- Ansible
- Chef/Puppet
Email Sent

Potential Malware/Ransomware Risk

octoblu-flow@webhook.octoblu.com
to me

Country: ES
Owner: ServiHosting Networks S.L.
Address: 185.22.92.100
Client: 10.11.6.101
URI: (BE CAREFUL CLICKING) fundeun.es/
See Results: https://www.virustotal.com/en/ip-address/185.22.92.100/information/
Quick Demo

DEMO
Why APIs are Important

- Allows you to thread disparate and/or complimentary data together
- Adds agility to your tools to exploit available open source Threat Intelligence
- Allows you to evaluate your transactions on premise instead of sending the data to the cloud
- Developers are able to build new solutions (mashups) never before envisioned
## DevOps/SecOps Demand (Indeed.com)

<table>
<thead>
<tr>
<th>Category</th>
<th>Demand</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cyber Security</strong></td>
<td>32000</td>
<td></td>
</tr>
<tr>
<td>Cyber Security SIEM</td>
<td>1133</td>
<td>3.54%</td>
</tr>
<tr>
<td>Cyber Security Firewall</td>
<td>2536</td>
<td>7.93%</td>
</tr>
<tr>
<td>Cyber Security Threat Intelligence</td>
<td>2671</td>
<td>8.35%</td>
</tr>
<tr>
<td>Cyber Security Intrusion</td>
<td>2100</td>
<td>6.56%</td>
</tr>
<tr>
<td>Cyber Security Python</td>
<td>1960</td>
<td>6.13%</td>
</tr>
<tr>
<td>Cyber Security JavaScript</td>
<td>940</td>
<td>2.94%</td>
</tr>
<tr>
<td>Cyber Security Devops</td>
<td>272</td>
<td>0.85%</td>
</tr>
<tr>
<td><strong>Threat Intelligence</strong></td>
<td>2671</td>
<td></td>
</tr>
<tr>
<td>Python</td>
<td>415</td>
<td>15.54%</td>
</tr>
<tr>
<td>Javascript</td>
<td>108</td>
<td>4.04%</td>
</tr>
<tr>
<td>Both</td>
<td>523</td>
<td>19.58%</td>
</tr>
</tbody>
</table>
You Need Intel, not Just Threat Intel!

- Threat Intel isn’t particularly valuable if you cannot mash it up with local Intel
- There are sources of local Intel available all around you
  - APM Tools
    - BMC
    - EdgeSight
    - Any agent based solution that writes data to an ODBC back end database.
  - Windows Log files
  - /var/log/
  - Packet captures
Key Take-Aways

- Even the best Threat Intel is less effective in the absence of local Intel.
- Local Intel is in multiple places often outside the security practice/portfolio.
  - APM tools that write to a database
  - PCAP captures from SPAN aggregators or SPAN vendors
- Teams need to embrace the DevOps/SecOps mindset.
  - Learn Python
  - Learn JavaScript
- The people with the skills you need are likely in your organization already.
Apply What You Have Learned

- Evaluate your team’s skills matrix
- Build development/coding skills within your teams
  - Python
  - Javascript
- Get an asset inventory of every tool or product that collects local Intel and determine how it can be exploited
- Add a developer to your team, be prepared to “deputize” the skills you need if you cannot hire them
Thank You!!
## Seminar Schedule

<table>
<thead>
<tr>
<th>Start Time</th>
<th>Title</th>
<th>Presenters</th>
</tr>
</thead>
<tbody>
<tr>
<td>11:25 AM</td>
<td>Closing the Gap Between Public and Private Threat Intelligence Sharing</td>
<td>Jason Smith, Sean Duca</td>
</tr>
</tbody>
</table>
Closing the Gap Between Public and Private Threat Intelligence Sharing

**Sean Duca**
Vice President
Regional Chief Security Officer – APAC
Palo Alto Networks
@SeanDuca

**Jason Smith**
Technical Director
CERT Australia
Australian Cyber Security Centre
Agenda

- How Far We’ve Come
- What & How We Share
- Use Cases – Energy & Financial Sector
- The Way Forward
How Far We’ve Come
How Far We’ve Come

- Challenges
  - TRUST
  - Nomenclature (syntax)
  - Meaning (semantics)
  - Infrastructure to facilitate sharing
  - Tooling to craft intel for sharing

- Lessons Learned
  - People are slow and error prone – who want to copy and paste bad IP’s!
  - We need to automate the mundane
Threat intelligence was the buzzword of 2016, but how did that play out?

- Garbage in and garbage out
- Difficulty making sense of all the feeds
- Shared sector & regional specific campaign info proved most valuable
- There's a need for standardized formats to ease monitoring & preventive countermeasures
Challenges & Resistance To Sharing
What We Need To Know & Share

- **Threat Indicators**: Forensic artifacts
- **Adversary’s Campaign Plan**: Threat indicators for each link in the cyberattack lifecycle
- **Context**: Additional non-campaign plan intelligence about an adversary group
- **Adversary Dossier**: Campaign plans + context
How Do We Express It In A Standard Format
What Is Being Shared

TTPs
• Tough!

Tools
• Challenging

Network/Host Artifacts
• Annoying

Domain Names
• Simple

IP Addresses
• Easy

Hash Values
• Trivial

NB. (TTP) Tactics, Techniques, and Procedures
What Is Being Shared

- Banking and finance
- Energy
- Communications
- International CERT
- Transport
- Defence
- Resources
- Vendor
- International ISAC
- Law Enforcement
- Law Enforcement
- Government
Use Case – Energy Sector
Use Case – Financial Sector
The Way Forward
The Way Forward

How you share with others

What it means if you find it

What to look for
Where To Start

MineMeld
https://github.com/PaloAltoNetworks/minemeld

CTI Toolkit
https://github.com/certau
Where To Start: MineMeld

3. Choose outputs

**High Confidence URLs**

Block these URLs through [URL Filtering](#).

**Low Confidence URLs**

Set a firewall alert for these URLs through [URL Filtering](#).

**High Confidence IP Addresses (Inbound)**

Use these as a Destination Address in a Security policy rule.

**High Confidence IP Addresses (Outbound)**

Use these as a Source Address in a Security policy rule.

**High Confidence Domains**

Use these domains for [DNS Sinkholing](#).

To use these as a destination or source IP address, add them to an [external dynamic list](#) or a [dynamic address group](#).
Where To Start: cti-toolkit

sources

cti-toolkit

outputs
Key Takeaways

- Learn from what we’ve seen work and not work
- Understand our adversaries – it’s half the battle
- Access information from valued sources, such as:
  - Use the data inside your own network
  - National or sector specific CERTs / ISACs
  - Sector-specific trust groups
  - Commercial feeds
- Intelligence must be acted on in a timely and effective manner
- Threat information needs to fit within the broader security workflows
Apply What You’ve Learned

● Immediate Action
  ● **Get involved!** Install / trial free open source solutions to help you ingest and action threat intelligence in a timely manner

● Within three months
  ● Identify communities to participate in – CERTs, ISACs, ISAOs, sector-specific and cross-sector
  ● **Identify intel of value** - what types of information you can action

● Within six months:
  ● **Share the lessons learned**
  ● Help break the adversary tradecraft - begin to share with others
Thank you