
27th ANNUAL
FIRST
CONFERENCE
BERLIN
14 - 19 JUNE 2015
UNIFIED SECURITY:
IMPROVING THE FUTURE

27th ANNUAL FIRST CONFERENCE BERLIN
14-19 JUNE 2015

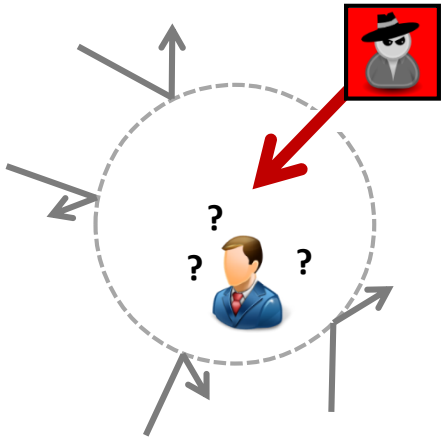
# At the Speed of Trust

## Moving to the left of “boom”

Wayne Boline (DSIE)
Denise Anderson (FS-ISAC)
George Johnson (NC4)

# Evolution of Cyber Security and the Cyber Intelligence Problem

## Yesterday's Security



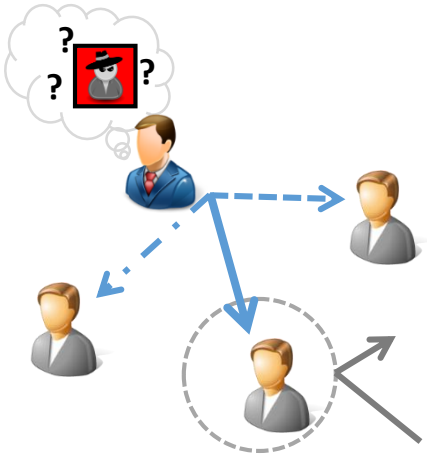
### Network Awareness

**Protect the perimeter** and patch the holes to keep out threats share knowledge internally.

### Increasing Cyber Risks

- Malicious actors have become much more sophisticated & money driven.
- Losses to US companies now in the tens of millions; WW hundreds of millions.
- Cyber Risks are now ranked #3 overall corporate risk on Lloyd's 2013 Risk Index.

## Today's Problem



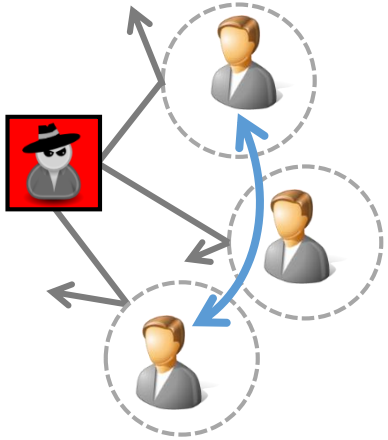
### Intelligence Sharing

Identify and track threats, incorporate knowledge and **share what you know manually** to trusted others, which Is extremely time consuming and ineffective in raising the costs to the attackers.

### Manually Sharing Ineffective

- Expensive because it is slow manual process between people.
- Not all cyber intelligence is processed; probably less than 2% overall = high risk.
- No way to enforce cyber intelligence sharing policy = non-compliance.

## Tomorrow's Solution



### Situational Awareness

**Automate sharing** – develop clearer picture from all observers' input and pro-actively mitigate.

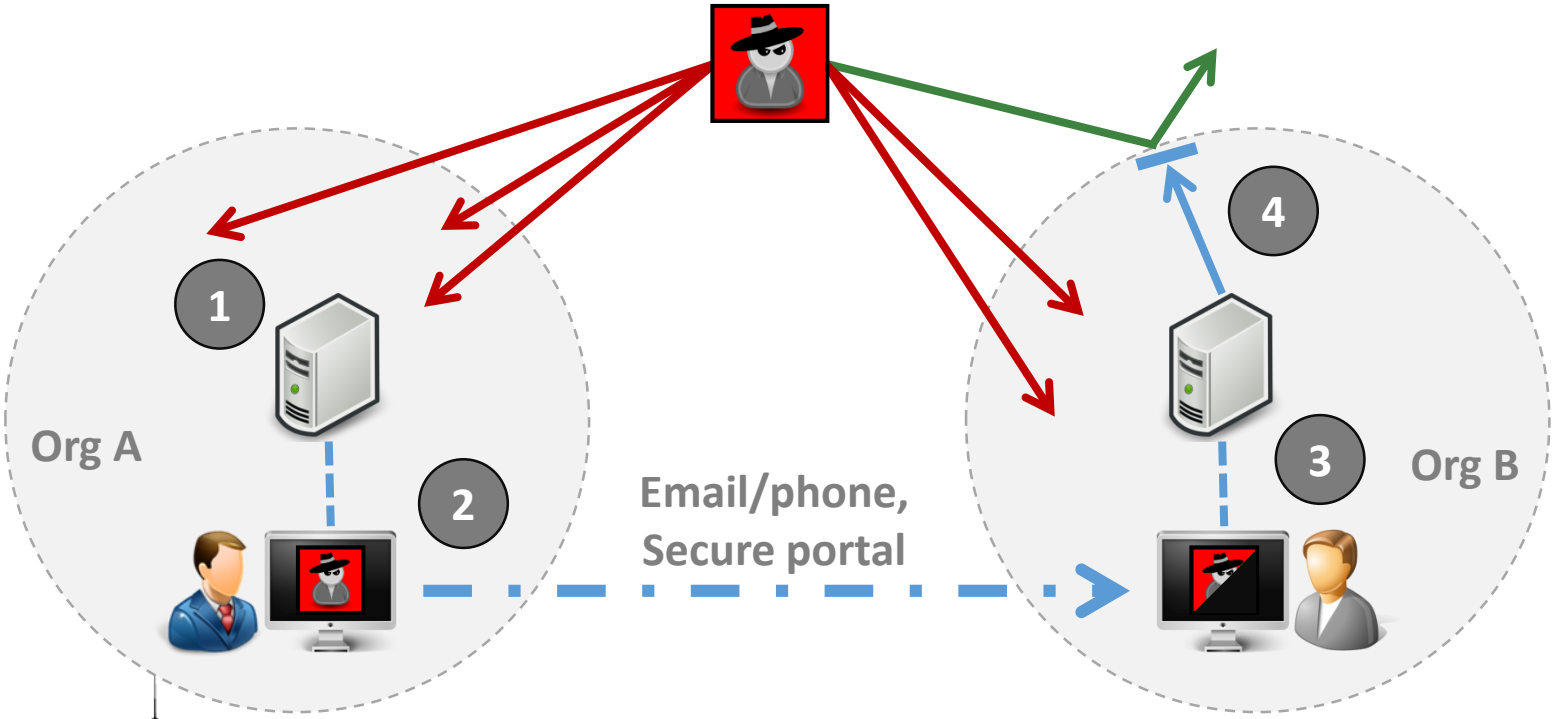
### Solving the Problem

- Security standards recently matured.
- Cyber Intelligence Sharing Platform revolutionizing sharing and utilization of threat intelligence.

# Cyber Intelligence Problem

## Typical Sharing of Intelligence Today

1. Machines detect threats, typically stored in proprietary formats or PDFs
2. People export data and manually share via multiple media types
3. Other people rarely get a full picture of ongoing threats
4. Only some threats are mitigated



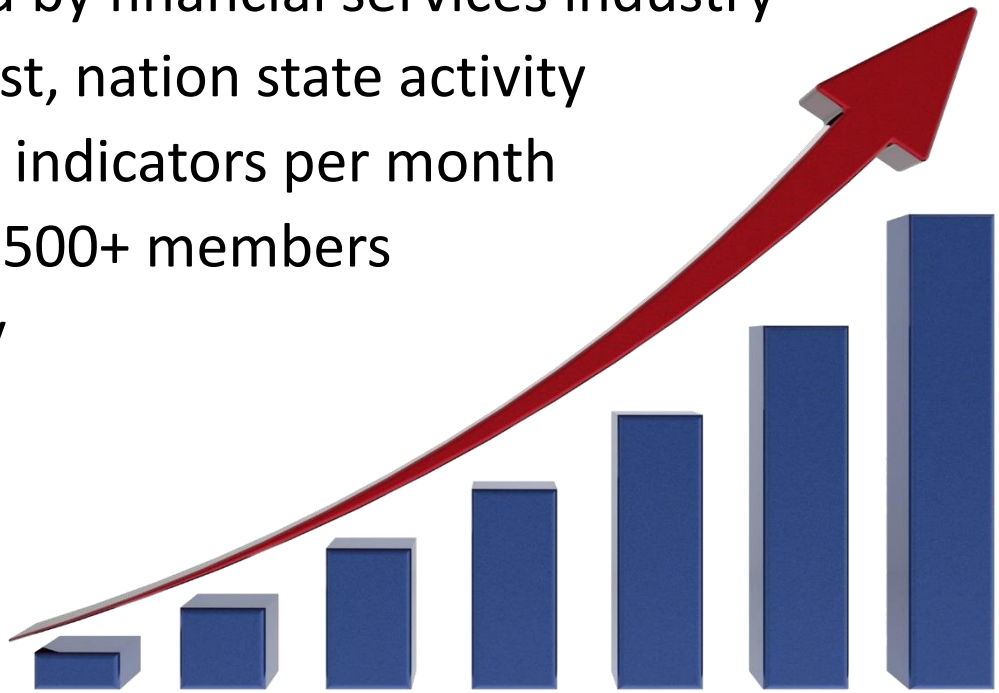
# Impediments To Progress

- Trust
  - isolated into “like” organizations based on similarly perceived threats/business line
  - Common/Standard rules on handling, marking, controls, and auditing – and how do we agree and share them?
- Vendor interoperability
- Individual organization with manual processes
  - What to share (Metadata, full data, full packet capture)
  - How to share (anonymous, attributable, what handling caveats, how to I capture and move the data to the sharing environment)
  - What to do with the data that I receive (is it actionable)
- Simplicity to support small organizations
- Shortage of skilled analysts
- How to share without tipping off the enemy?
- Senior leadership awareness, understanding, and support

# FS-ISAC MISSION:

## Sharing Timely, Relevant, Actionable Cyber and Physical Security Information & Analysis

- A nonprofit private sector initiative formed in 1999
- Designed/developed/owned by financial services industry
- Mitigate cybercrime, hactivist, nation state activity
- Process thousands of threat indicators per month
- 2004: 68 members; 2015: 5,500+ members
- Sharing information globally



FINANCIAL SERVICES ISAC

# FS-ISAC Operations

**Information Sources**

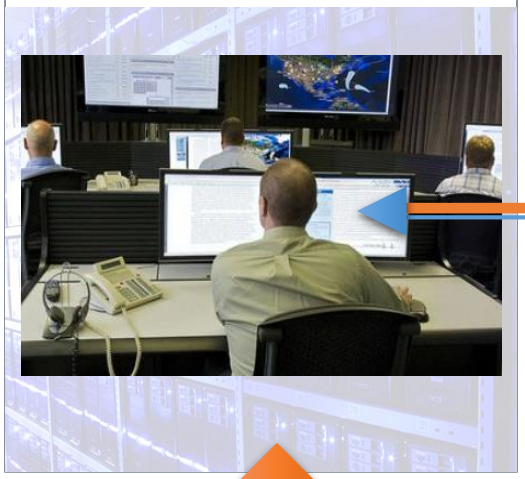
**GOVERNMENT SOURCES**

- DHS
- Treasury & FS Regulators
- FBI, USSS, NYPD
- Other Intel Agencies

**PRIVATE SOURCES**

- iSIGHT Partners Info Sec
- Secunia Vulnerabilities
- Wapack Labs Malware Forensics
- NC4 Phy Sec Incidents
- MSA Phy Sec Analysis

**FS-ISAC 24x7 Security Operations Center**



**SECTOR SOURCES**

- **FS-ISAC Members**
- Cross Sector (other ISACS)
- Open Sources (Hundreds)

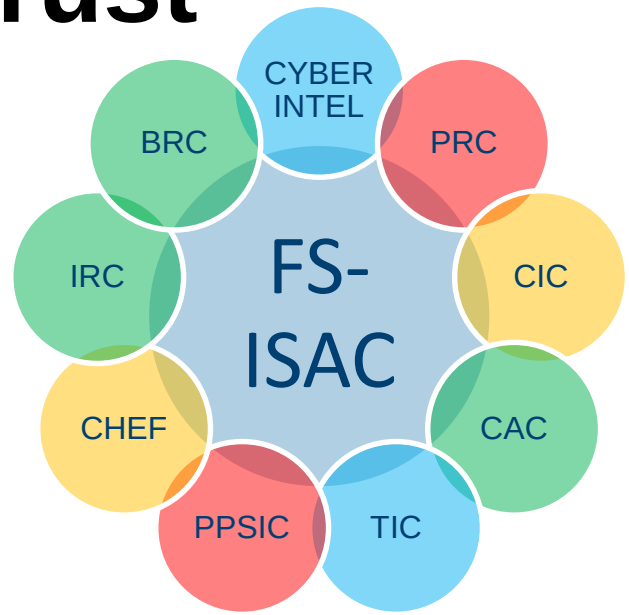
**Member Communications**

- Information Security
- Physical Security
- Business Continuity/ Disaster Response
- Fraud Investigations
- Payments/ Risk

Alerts

Member Submissions

# How FS-ISAC Works: Circles of Trust




- Clearing House and Exchange Forum (CHEF)
- Payments Risk Council (PRC)
- Payments Processor Information Sharing Council (PPISC)
- Business Resilience Committee (BRC)
- Threat Intelligence Committee (TIC)
- Community Institution Council (CIC)
- Insurance Risk Council (IRC)
- Compliance and Audit Council (CAC)
- Cyber Intelligence Listserv
- Education Committee
- Product and Services Review Committee
- Survey Review Committee
- Security Automation Working Group (SAWG)

**Member Reports Incident to Cyber Intel list, or via anonymous submission through portal** → **Members respond in real time with initial analysis and recommendations** → **SOC completes analysis, anonymizes the source, and generates alert to general membership**

# Traffic Light Protocol (TLP)

- Restricted to a defined group (e.g., only those present in a meeting.) Information labeled **RED** should not be shared with anyone outside of the group
- **AMBER** information may be shared with FS-ISAC members.
- **GREEN** Information may be shared with FS-ISAC members and partners (e.g., vendors, MSSPs, customers). Information in this category is not to be shared in public forums
- **WHITE** information may be shared freely and is subject to standard copyright rules
- Within communities is manageable
- Across communities is hard and requires ongoing effort (call to action)

# Alert Profile Configuration

NOTIFICATION ALERT PROFILES

Individual email addresses can be configured with different alert preferences. Select an email address to view or change preferences. Click the Add or Delete icon to further manage your preferences.

Email Address: travis.brown@nc4.us

Save Cancel

## FS-ISAC Alert Types

Select the FS-ISAC content types for which you wish to be alerted.

- [x] Announcements
- [x] CISCP Reports (5 selected)
- [x] Collective Intelligence Reports (32 selec...
- [x] Cyber Incidents
- [x] Cyber Threats
- [x] Cyber Vulnerabilities
- [x] Physical Incidents
- [x] Physical Threats
- [x] Requests For Information

# Information Sharing & Analysis Tools

**Threat Data, Information Sharing**

- **Anonymous Submissions**
- **CyberIntel Listserver**
- Relevant/Actionable Cyber & Physical Alerts (Portal)
- **Special Interest Group Listservers (Community Institution Council)**
- Document Repository
- Member Contact Directory
- Member Surveys
- Risk Mitigation Toolkit
- Threat Viewpoints

**Ongoing Engagement**

- Bi-weekly Threat Calls
- Emergency Member Calls
- Semi-Annual Member Meetings and Conferences
- Regional Outreach Program
- Bi-Weekly Educational Webinars

**Readiness Exercises**

- US and EU Government Sponsored Exercises
- **Cyber Attack against Payment Processes (CAPP) Exercise**
- Advanced Threat/DDoS Exercise
- Industry exercises-Systemic Threat, Quantum Dawn Two, etc.

DSIE Defense Security Information Exchange

# WHO ARE WE?

- DSIE member organizations represent the major US Defense Industrial Base (DIB) companies and key DIB supply chain partners.
- We have been aggressively and continuously targeted by determined Nation State APT (Advanced Persistent Threat) adversaries since at least 2003.
- A decade+ of APT Cyber-Threat prevention, detection, mitigation, and remediation has produced arguably the most experienced APT Cyber-Threat analysts, network/system engineers, thought leaders, and practitioners in the world

**OUR SUCCESS IS BUILT THE DEMONSTRATED VALUE OF REAL-TIME SHARING OF "RAW" INTELLIGENCE, ACTIVE ENGAGEMENT & COLLABORATION AS SOON AS POSSIBLE IN THE KILL CHAIN**

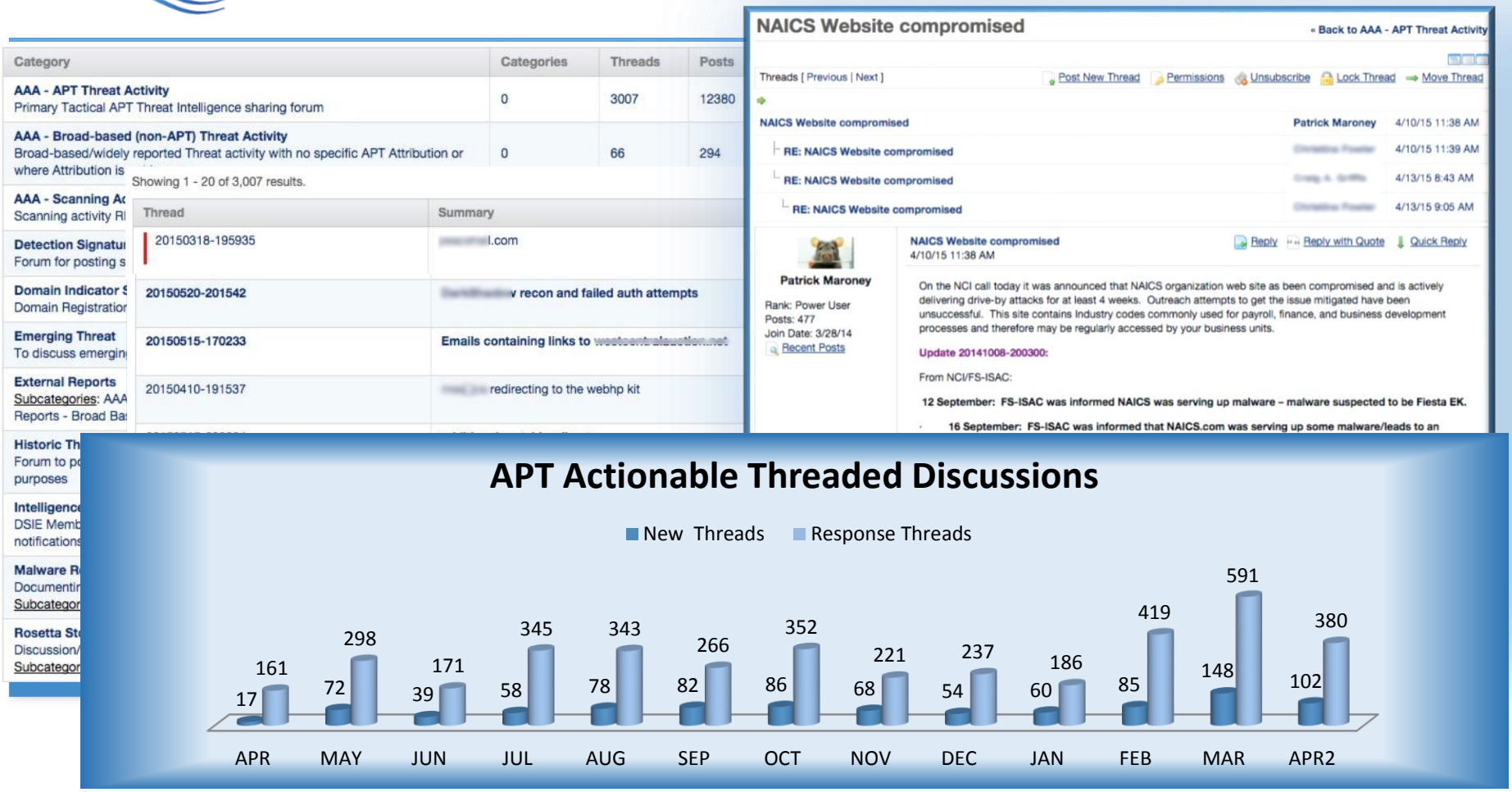
**...AND MOST IMPORTANTLY THE TRUST THAT IS REQUIRED TO SHARE ATTRIBUTIONAL DATA**

DSIE Defense Security Information Exchange

# WINS

- Trusted exchange – 7+ years
- Timeliness is preventing losses
- Beyond indicators - building community view of adversaries
  - WIKIs
  - CRITs
- Analyst community bonding:
  - DSIE Live! – Analyst Driven Conferences
  - Bi-Weekly Analyst Calls
- Facilitate TechEx and collaboration among analysts
- Train analysts across DIB
- Tools & Frameworks Working Groups
- Develop cutting edge intel processes and tools
- Promote best practices

# Portal Threaded Discussions




## APT Actionable Threaded Discussions

# DSIE Live! - Analyst Driven Conferences

## Breakout Sessions

▼ Threads

| Thread |
| --- |
| DIB ISAO Strategic Plan - Analyst Engagement |
| Command Wrapper |
| Running Phishing exercises to raise end-user av |
| Topic - Incident Response in the Cloud |
| Crimeware - To Catch a Thief |
| pDNS management |
| Friday Afternoon Breakout Session Opportunitie |
| Swarm Creativity: Collaborative Innovation Netw |

## SMECON & BOFCON

▼ Threads

Showing 15 results.

| Thread |
| --- |
| SMECON/BOFCON Concept & Instructions |
| Where's Waldo |
| Stucco Situation & Threat Understanding by C Contextual Observati |
| Orange Data Analytics |
| BOFCON session |
| BOFCON - Automation Domination |
| ACIX Initiatives |
| FireEye SMECON |
| Malware Analysis |

## Finalized Sessions

▼ Threads

Showing 19 results.

| Thread | Date |
| --- | --- |
| Campaign Overview | Day 2 - Thur A |
| LM-CIRT's solution to static malware analysis and metadata collection | Day 1 - Wed A |
| **Incident Response - It's Not Rocket Surgery (but it's hard)** | **Day 3 - Fri Ap** |
| **Android, Python, Java, 0day, oh my. What's hot in delivery methods.** | **Day 2 - Thur A** |
| **User-Agents & X-Mailers** | **Day 2 - Thur A** |
| **Indicator Enrichment (LM DigiMon)** | **Day 3 - Fri Ap** |
| pDNS management | Day 2 - Thur A |
| **Straight Thuggin** | **Day 2 - Thur A** |
| **Analytic Objectivity** | **Day 2 - Thur A** |

# Collaboration Features

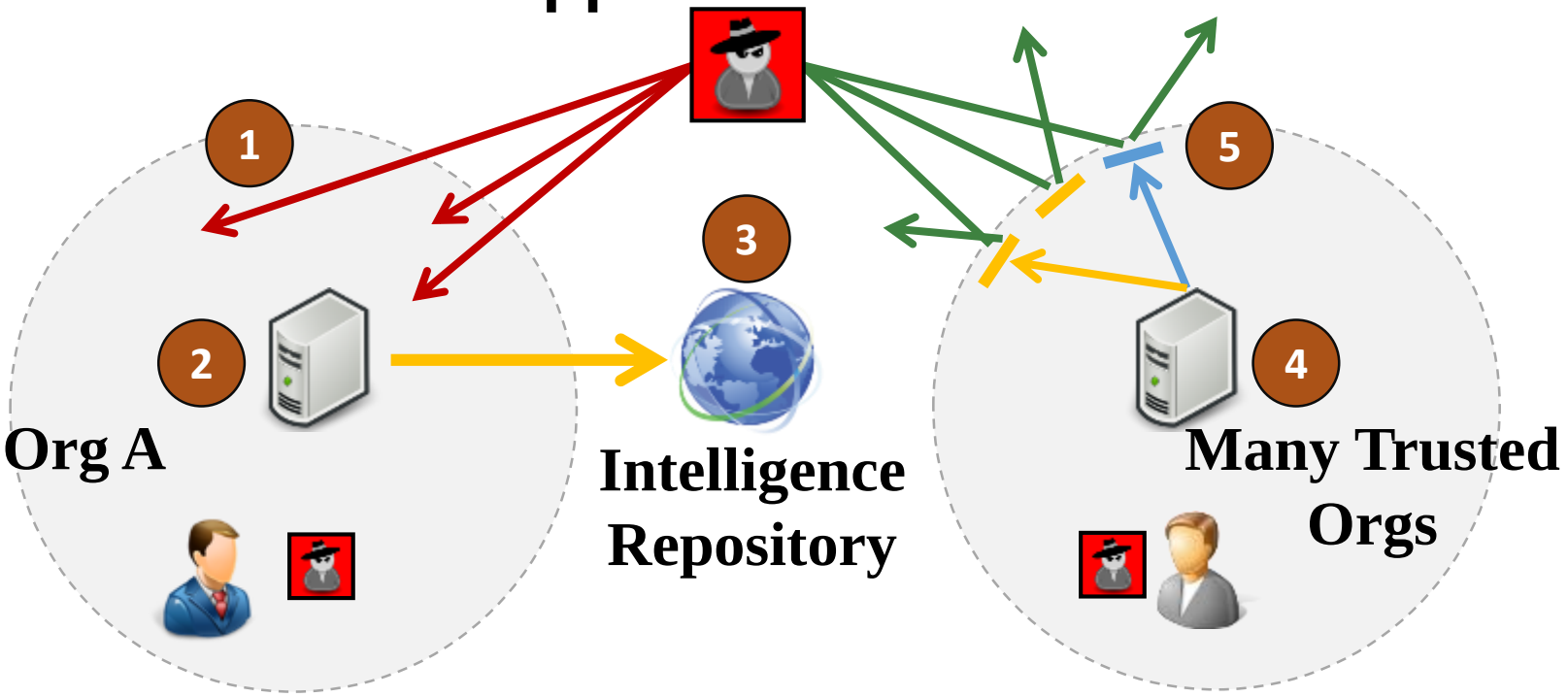

Document mgmnt
Secure messaging
Secure chat
Message Boards
Wikis
Blogs
Shared calendars
Custom web content
Rigorous security
RSA 2-factor auth.
Compartments
Traffic light protocol labels
Robust auditing
Administrative tools
Membership & roles mgmnt
Granular permissions
Anonymous posts
Notifications
X-application search
Forms and lists
Member directory
Task lists
Member survey
Announcements
Alerts app
Activities & statistics
Universal tagging
Universal categorization
Comments, ratings, & flags
Tag clouds
Flexible layouts
Media gallery

# Analyst Driven Security Automation


**Will Revolutionize Information Sharing**

# Sharing Solution

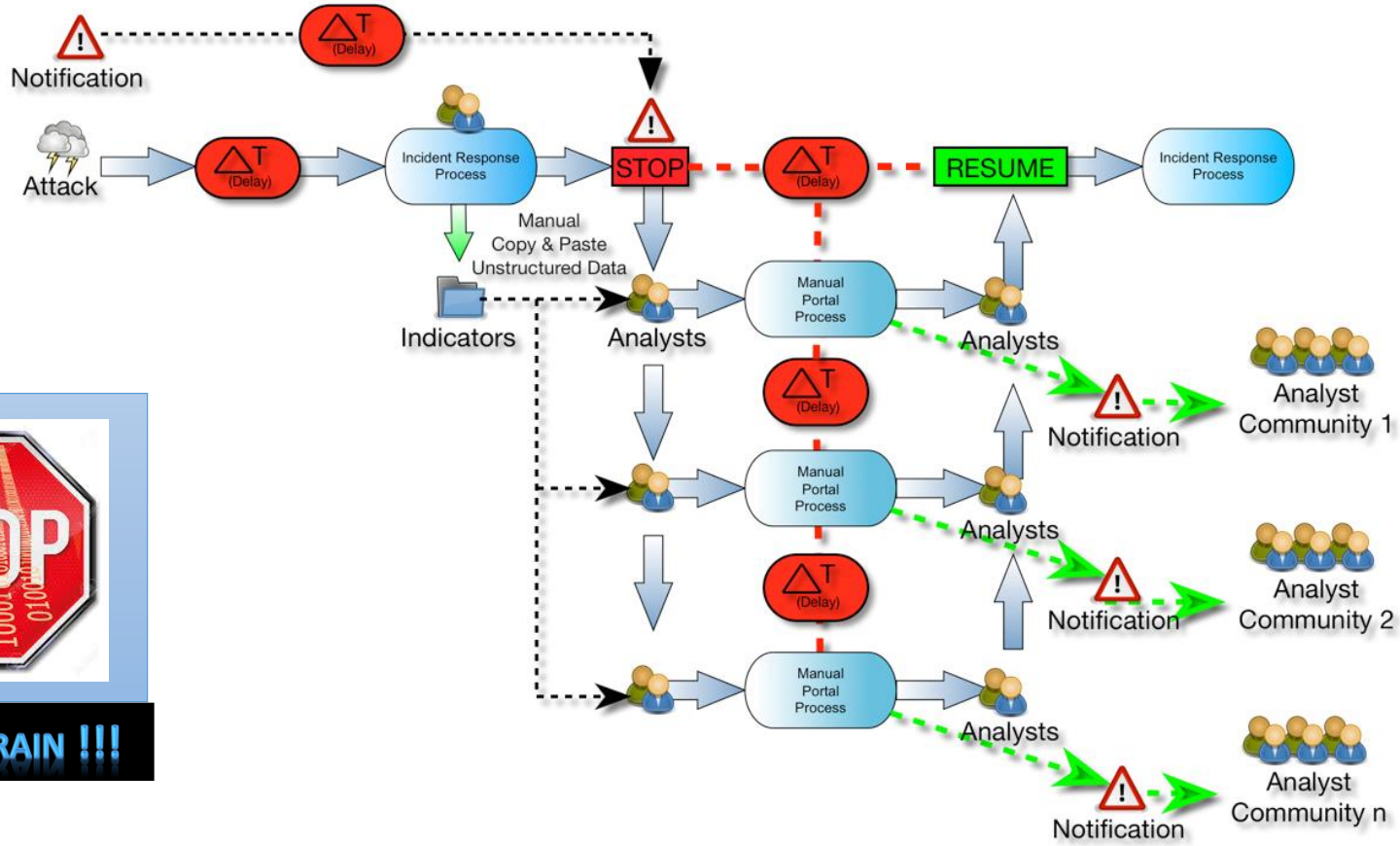
- **Instead of 2% or less of attacks blocked, detected, or prevented, a much higher percentage of attacks are stopped**



# We Don’t Need Another Portal*

*(* Sung to the tune of Tina Turner’s Classic Song from Road Warrior)*

## Current Manual Process - Multiple Portals




# Information flows accelerate

- 1,554 installations of Soltra Edge
- 12,000,000 indicators in FS-ISAC repository
- 10,000 daily requests for information from FS-ISAC repository
- Are we succeeding to death?
- How do we prevent automation from becoming part of the problem?

# Common Language(s)


- **OASIS CTI**
  - New International Standard for Cyber-Threat Intelligence Inter-Exchange
  - Based on DHS/MITRE STIX/CybOX/TAXII
  - Extension Data Models for OASIS CIQ, CAPEC,MAEC, OpenIOC, OVAL, Snort, Yara, CVRF
  - Widely deployed in select communities
  - Significant momentum in Vendor and Open Source Communities
  - Many tools for converting de facto formats (e.g., CIF, OpenIOC, VERIS)
- Other Emerging Standards
  - **IETF IODEF**
  - **OMG Threat/Risk** and **SIMF**

# Cyber Threat Intelligence

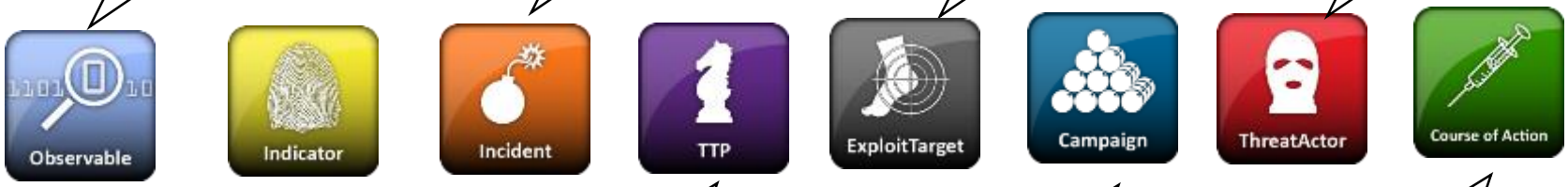
## Consider These Questions…..

What **Activity** are we seeing?

Where has this threat been **Seen**?

What weaknesses does this threat **Exploit**?

**Who** is responsible for this threat?



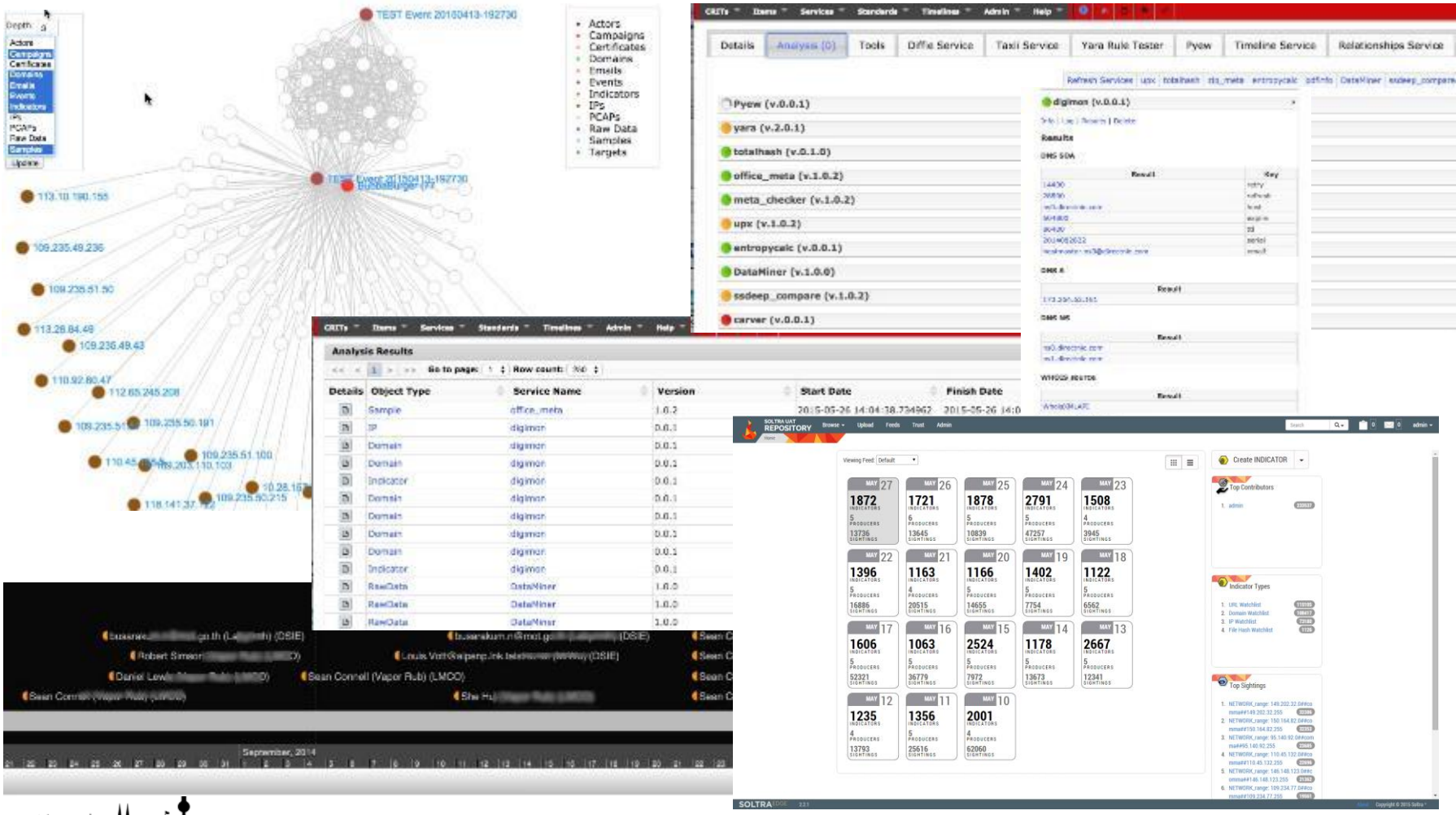

What **Threats** should I be looking for and why?

What does it **Do**?

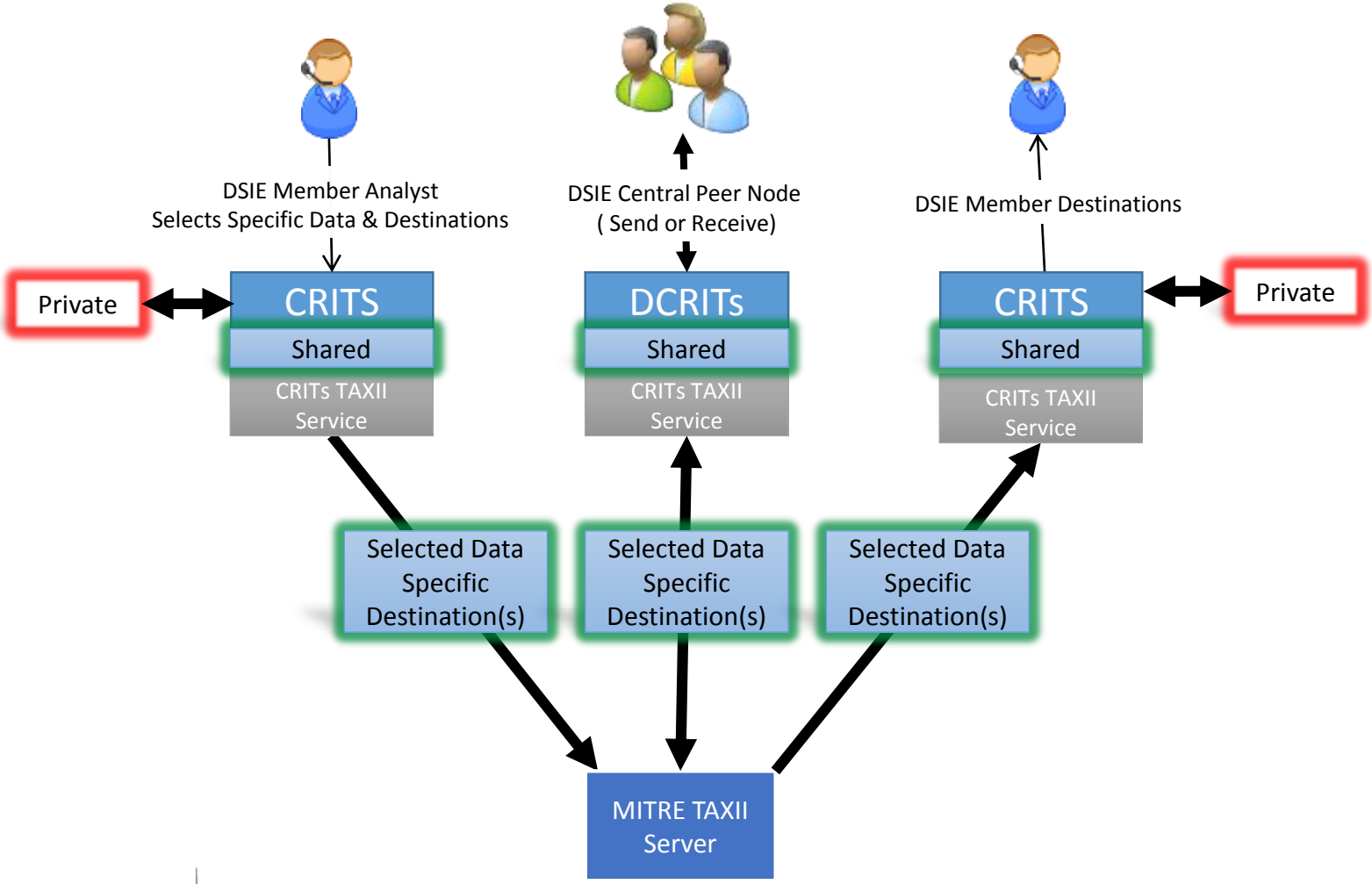
**Why** does it do this?

**What** can I do?

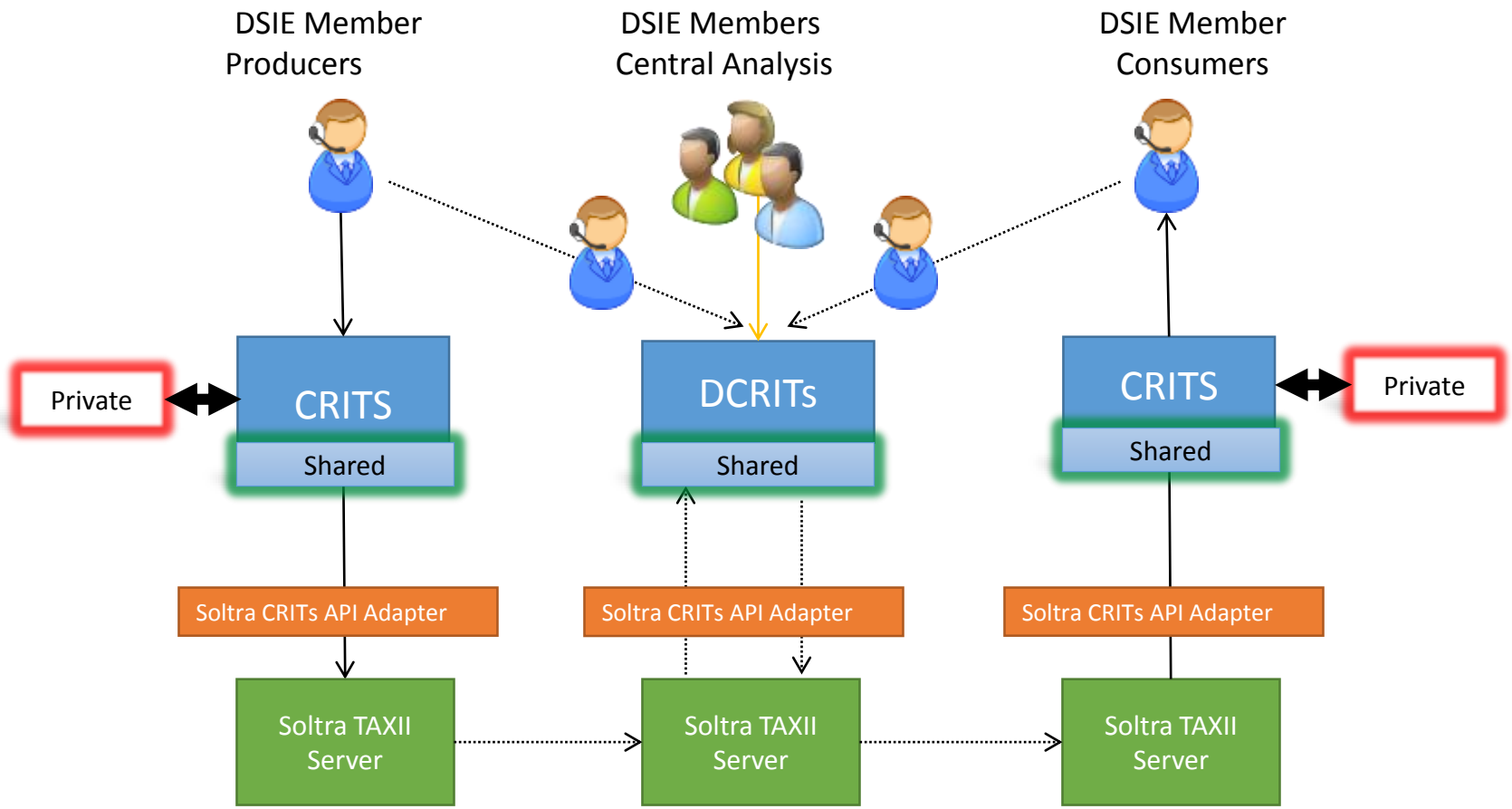
# Real Automation In Use



# Analyst Driven: CRITs-TO-CRITs

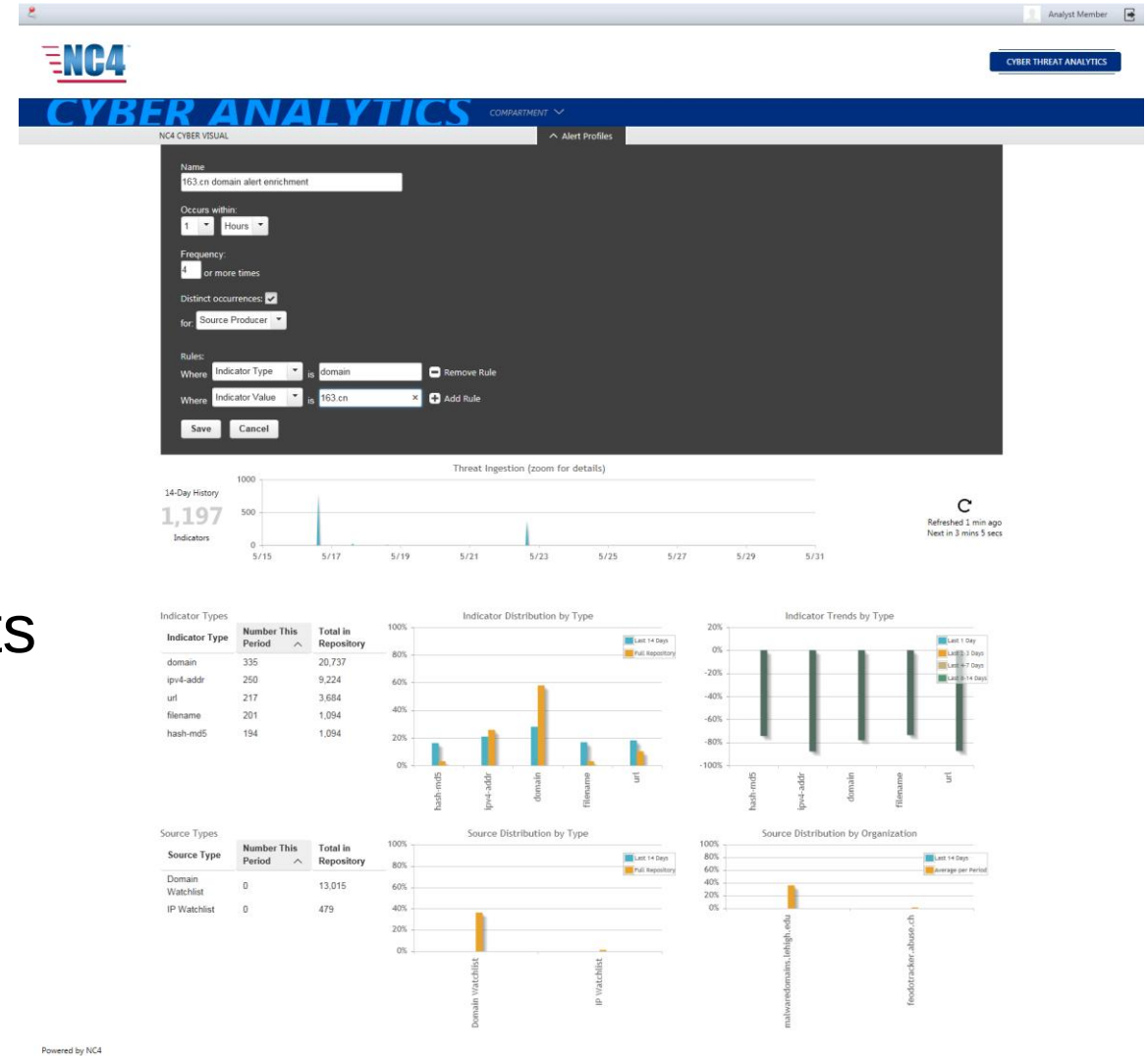


# Standards Based Automated Sharing



# Making it Actionable

- Rule builder for alerts
- Flexible visualization framework based on splunk for analytics
- Portlet in portal meant for Analysts
- Road map for Campaigns, Actors, TTP's, etc…



# Automation Maturity

- Humans will always be in the loop...
  ...but Analyst Driven Automation will replace many current manual processes
- Using STIX and TAXII gateways (aka OASIS CTI) we can leverage already scarce talent
- Fewer analysts will have to develop their own signatures
- Using automation it is possible to move signatures faster
- Off the shelf COTS may not interoperate across vendors
- Open Source may require in-house development to automate information flow
- But, can you trust Analysts/Incident Handlers in other organizations?

# What You Can Do

- Continue working on agreement of handling protocols (TLP, Data Marking)
- Continue working on defining Relevancy to prevent the “firehose” effect
- Encourage Cyber Observable/Indicator sharing within your organization
- Work within standards that are widely adopted (e.g., OASIS CTI, IODEF)
- Don’t wait for the perfect solution – start now and help mature the process
- Engage with working and sharing groups
  - Software Supply Chain Assurance
    - https://buildsecurityin.us-cert.gov/
  - Open Web Application Security Project
    - http://www.owasp.org
  - ISAC – find one that you fit
  - SANS/DSHIELD

# Questions?

# References

- TAXII: Trusted Automated eXchange of Indicator Information (http://taxii.mitre.org)
- CRITS: Collaborative Research Into Threats (https://crits.github.io/)
- YETI: An open source proof-of-concept of TAXII (https://github.com/TAXIIProject/yeti)
- STIX: Structured Threat Information eXpression (https://stixproject.github.io/)
- CYBOX: Cyber Observable eXpression (http://cybox.mitre.org)
- CAPEC: Common Attack Pattern Enumeration and Classification (http://capec.mitre.org)
- MAEC: Malware Attribute Enumeration and Characterization (http://maec.mitre.org)
- CVE: Common Vulnerability Enumeration (http://cve.mitre.org)
- CWE: Common Weakness Enumeration (software typically) (http://cwe.mitre.org)
- OVAL: Open Vulnerability and Assessment Language (http://oval.mitre.org)
- TLP: Traffic Light Protocol (TLP) Matrix & FAQ (http://www.us-cert.gov/tlp)
- OASIS – CIQ Entity Models (http://docs.oasis-open.org/ciq/v3.0/prd03/specs/ciq-specs-v3-prd3.html )
- CVRF - The Common Vulnerability Reporting Framework (http://www.icasi.org/cvrf )
- OASIS CTI TC (https://www.oasis-open.org/)
- IETF IODEF (https://datatracker.ietf.org/doc/draft-ietf-mile-rfc5070-bis/)
- OMG Threat/Risk (http://threatrisk.org/)

# CRITs

CRITs is an open source malware and threat repository that leverages other open source software to create a unified tool for analysts and security experts engaged in threat defense.

It has been in development since 2010 with one goal in mind: give the security community a flexible and open platform for analyzing and sharing threat data.

CRITs is free and open source, and can provide organizations around the world with the capability to quickly adapt to an ever-changing threat landscape.

CRITs can be installed locally for a private isolated instance or shared among other trusted organizations as a collaborative defense mechanism.

CRITs support for OASIS CTI TC Standards (aka STIX CybOx, and TAXII) provide the foundations of the DSIE ACIX (Automated Cyber-intelligence Inter-Exchange) Initiatives which will provide “Analyst Driven” Threat Intelligence dissemination to both Human Analysts and emerging Automation Processes that leverage Standards based structured threat intelligence.

Community Developed CRITs Services Extensions

- OPSWAT_Service
- anb_service
- carver_service
- chminfo_service
- chopshop_service
- clamd_service
- crits_scripts
- cuckoo_service
- data_miner_service
- diffie_service
- entropycalc_service
- farsight_service
- machoinfo_service
- meta_checker
- metacap_service
- office_meta_service
- opendns_service
- passivetotal_service
- pdfinfo_service
- peinfo_service
- pyew
- pyinstaller_service
- relationships_service
- shodan_service
- snuggiefish_service
- ssdeep_service
- stix_validator_service
- taxii_service
- threatgrid_service
- threatrecon_service
- timeline_service
- totalhash_service
- unswf_service
- upx_service
- virustotal_service
- whois_service