RSAConference2015
Singapore | 22-24 July | Marina Bay Sands

CHANGE
Challenge today's security thinking

SESSION ID: GRM-R09

# Threat Forecasting
## (Leveraging Big Data for Predictive Analysis)


**David DeSanto**

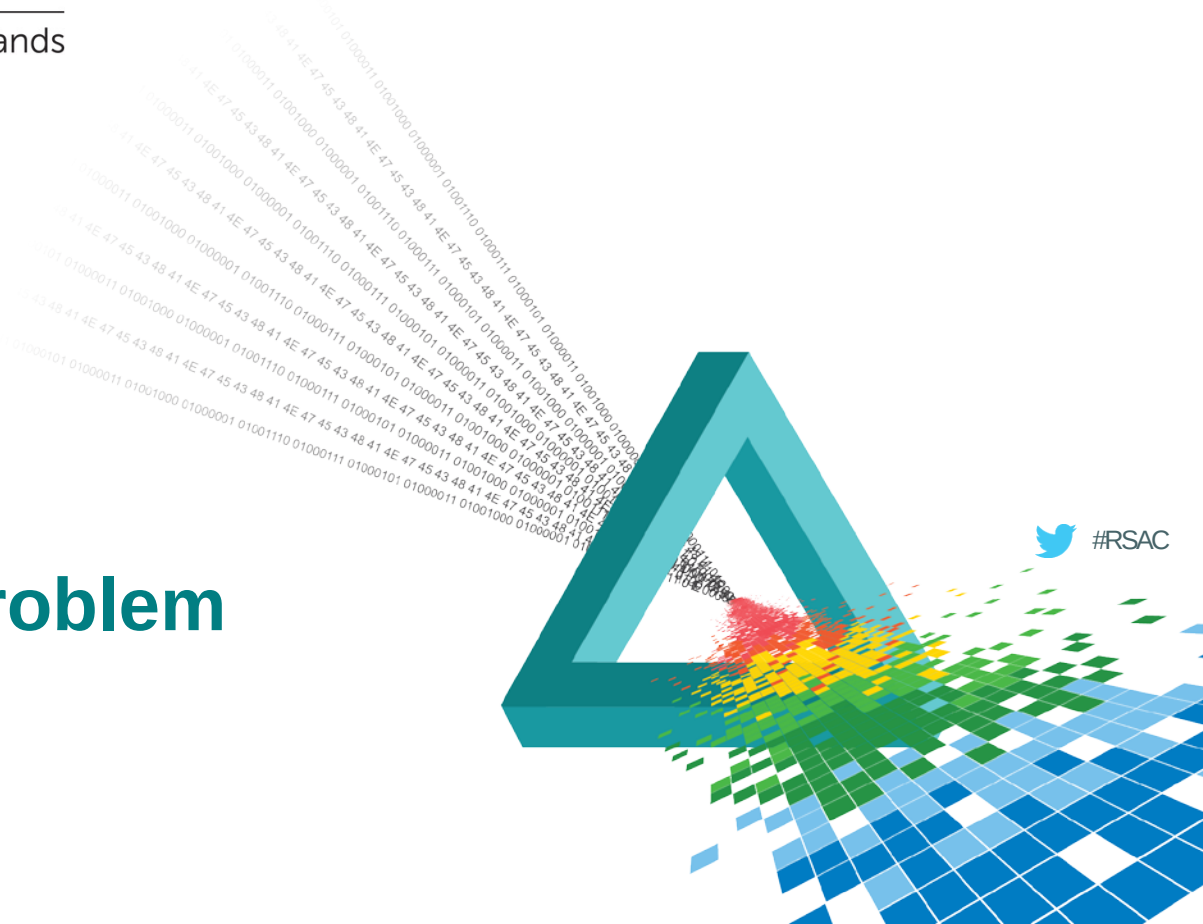
Director, Product Management
Spirent Communications, Inc.
@david_desanto


SPIRENT

#RSAC

# Agenda

- Identifying The Problem
- Threat Forecasting
- Threat Intelligence Feeds
- Community Sharing
- Connecting The Dots





# Identifying The Problem

SPIRENT

# Identifying The Problem

- Reviewing only historical threat reporting
  - Discusses what happened in the past
  - May have predictions about expected trends however these are expectations
  - A snapshot in time, not what is happening right now
- This doesn't mean to NOT look at these reports as they contain valuable trend data
  - Verizon DBIR (highly quoted)
  - Many vendors also produce reports (examples include Cisco, Mandiant)

# Identifying The Problem

- Security product limitations / effectiveness

| | All Programs | Anti-Virus | Network Firewall | Web App Firewall | Network IPS | IPSec VPN | SSL VPN | Custom Testing |
|---|---|---|---|---|---|---|---|---|
| Percentage of products that attain certification in the first cycle of testing | 4% | 27% | 2% | 0% | 0% | 0% | 0% | 0% |
| Percentage of products that eventually attain certification | 82% | 92% | 86% | 100% | 29% | 90% | 91% | 87% |
| Number of testing cycles typically required before products attain certification | Typically 2-4 cycles | | | | | | | |

**96% of product fail their first time to meet all testing requirements**

SPIRENT

**Certification Testing Passing Rate**

Source – ICSA Labs Product Assurance Report

# Identifying The Problem

- Security product limitations / effectiveness

| | All Programs | Anti-Virus | Network Firewall | Web App Firewall | Network IPS | IPSec VPN | SSL VPN | Custom Testing |
|---|---|---|---|---|---|---|---|---|
| **Percentage of products that exhibit violations during post-certification testing** | **36%** | **30%** | **18%** | **50%** | **93%** | **24%** | **27%** | **11%** |
| **Percentage of products that lose certification** | **13%** | **13%** | **3%** | **20%** | **43%** | **6%** | **9%** | **0%** |

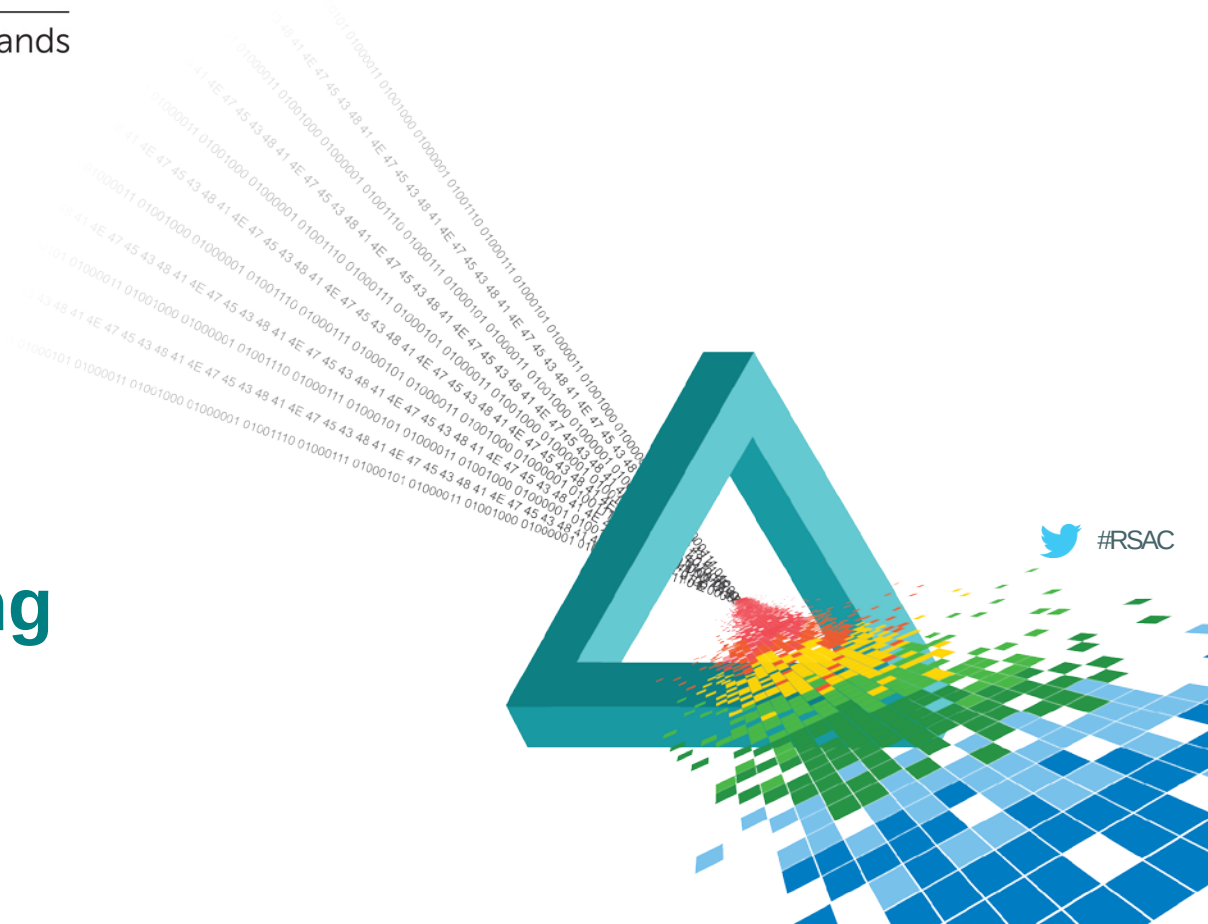
**Over 60% of products fail to meet all testing requirements when retested**

## Results For Post-Certification Testing

Source – ICSA Labs Product Assurance Report

RSAConference2015

Singapore | 22-24 July | Marina Bay Sands




# Threat Forecasting

SPIRENT

# Threat Forecasting

- Apply real-world threat intellegence with data collected within your organization to identify patterns or trends “in-the-wild” that may impact your organization
- How does it work?
  - Identify knowledge elements within your data and collect for tracking / reporting
  - Subscribe to threat intellegence feeds to get a holistic view of the greater threat landscape
  - Combine all datasets togther and use identified trends to determine high risk elements and provide protection to needed areas prior to attack / breach


SPIRENT

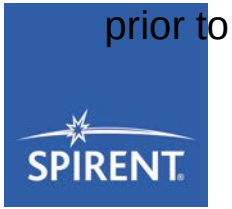
# Threat Forecasting

## Threat Forecasting

- Leverages your data for better accuracy to your organization
- Leverages third party intelligence to provide a holistic view of the entire threat landscape
- Shows what it happening today in the real-world (even within your industry vertical)
- Can help you improve your security posture prior to an attack or a data breach

## Historical Threat Reporting

- Overview of what happened within the period of time the report covers
- Sometimes provides predictions based on the upcoming year based on previous year trends
- Static report generated on a fixed schedule (usually once a year)
- No ongoing updates about how your organization maps to the threats occurring “in-the-wild”



# Threat Forecasting

**Knowledge Elements**

- Indicators of Compromise (IOCs)
  - IP address
  - URL (potentially FQDN + path)
  - MD5 Hash of a file
  - File
  - Win Registry Key
  - Win Driver
- Indicators of Interest (IOIs)
  - HTTP session
  - DNS Query
  - X509 Certificate
  - User account
  - Country of operation
  - Packet capture

RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

#RSAC

# Threat Intelligence Feeds

SPIRENT

# Threat Intelligence Feeds

- Community Driven and Commercial Offerings Available
- Most use industry accepted content formats
  - Data driven frameworks in XML, JSON, etc.
- Items to consider when choosing intelligence feeds
  - Update Frequency
  - Source of feed is within industry vertical
  - Quality of the intelligence feed
  - Popularity within the Information Security community
  - Ease of integration into tools already in use by IT / Ops Team

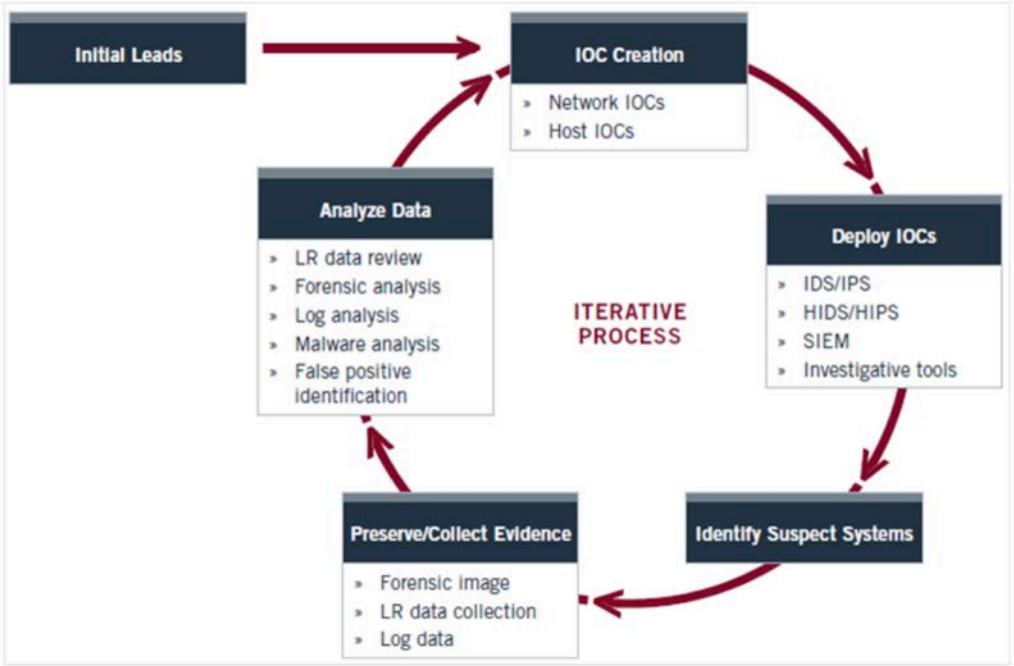
SPIRENT

# Threat Intelligence Feeds

## The Open Indictors Of Compromise Framework (OpenIOC)

- Open source framework developed by Mandiant (now FireEye)
- Started as internal project to help Mandiant rapidly search through security intelligence
- Goals of framework were to express
  - Components of an attack
  - Attack methodology
  - Evidence of a compromise
- Built as an extensible XML schema
  - To provide a way to share/digest threat intelligence as quickly as possible.
  - Easily machine-digestible for faster dissemination into the community.
- Resources
  - OpenIOC Framework – http://www.openioc.org

# Threat Intelligence Feeds




## OpenIOC - Create and Refine IOCs

Source – White Paper: An Introduction to OpenIOC, OpenIOC Framework (Mandiant, Inc.)

# Threat Intelligence Feeds

**Trusted Automated eXchange of Indicator Information (TAXII)**


- Initially launched in 2013
- Current Specifications v1.1
- XML structured framework
- Designed to run over HTTP (HTTPS)
- Design to deliver threat intelligence
  - Leveraged by other threat intelligence feeds and included within TAXII as a “payload”

- Resources
  - TAXII website – https://taxii.mitre.org
  - TAXII Community – http://taxii.mitre.org/community/
  - TAXII GitHub Repository – http://taxiiproject.github.io

# Threat Intelligence Feeds

## Structured Threat Information Expression (STIX)


- Initially launched in 2012
- Current Specifications v1.1.1
- XML structured framework
- Leverages TAXII for delivery

- Founded with six guiding principles
  - Provide coverage across the entire cyber security domain
  - Integrate, either directly or loosely, with other threat intelligence expression languages
  - Provide as much flexibility as possible in reporting knowledge elements
  - Supporting automation through maximizing structure and consistency
  - Needs to be human-readable as well

# Threat Intelligence Feeds

## Structured Threat Information Expression (STIX)


- Other threat intelligence expression languages supported
  - Cyber Observable eXpression (CybOX)
  - Common Attack Pattern Enumeration and Classification (CAPEC)
  - Malware Attribute Enumeration and Characterization (MAEC)
- Resources
  - STIX website – http://stix.mitre.org
  - STIX Community – http://stix.mitre.org/community/
  - STIX GitHub Repository – https://github.com/STIXProject/

# Threat Intelligence Feeds

## Cyber Observable eXpression (CybOX)

- Observable set of characteristics that express the observation of an event
- Initially launched in 2011
- Current Specifications v2.1
- XML structured framework
  - Includes pre-defined object representations
- Leveraged by STIX for cyber indicators

- Resources
  - CybOX website – http://cybox.mitre.org
  - CybOX Community – http://cybox.mitre.org/community/
  - CybOX GitHub Repository – https://github.com/CybOXProject/

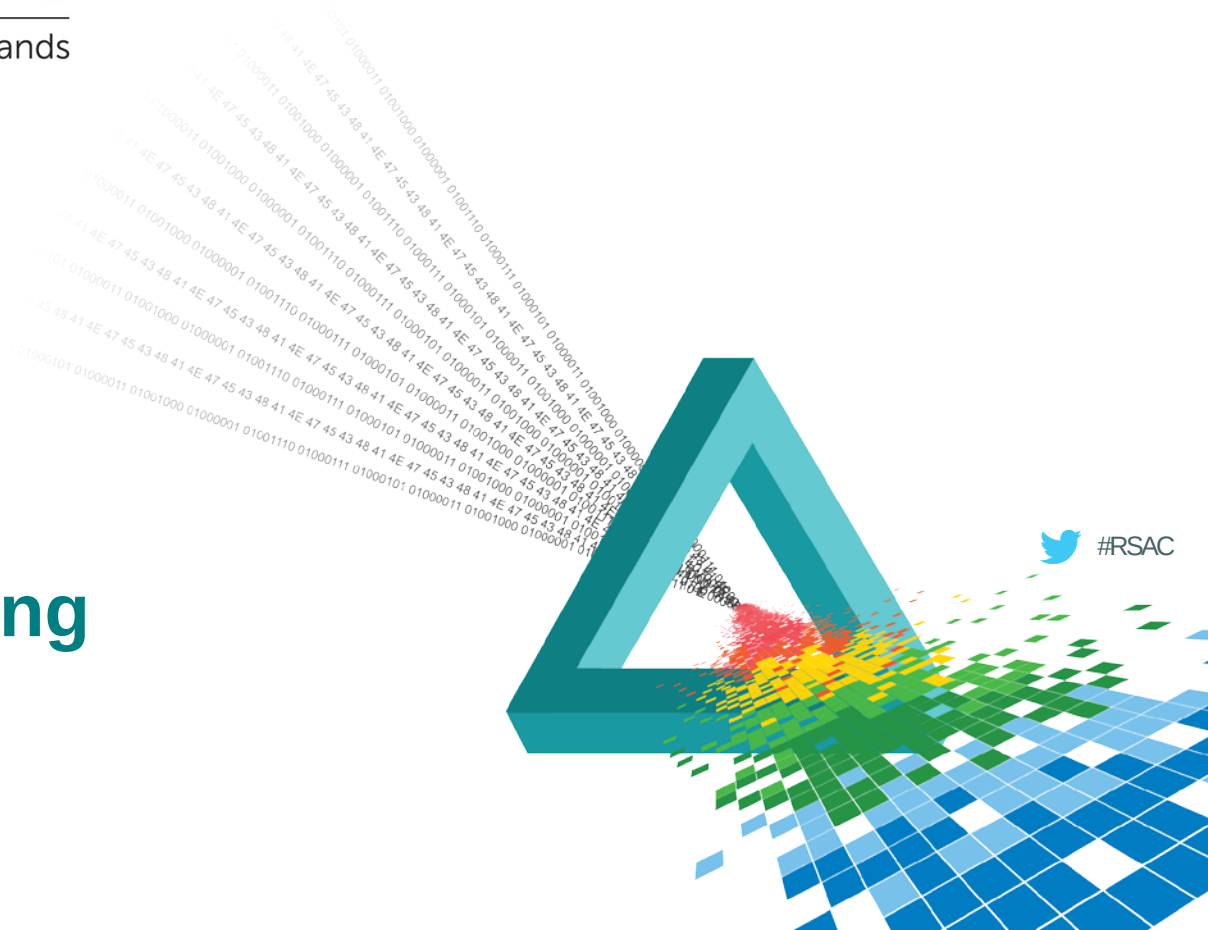
# Threat Intelligence Feeds

- Commercial Offerings
  - Different types available today
  - Before choosing a commercial offering, ask yourself
    - Is industry specific threat intelligence important?
    - What is provided within the commercial offering? Will it be easy to automate processing of?
    - Do you want an end-to-end solution that may not integrate with other solutions easily?
  - This may be the right choice for your organization depending on the size of your team

SPIRENT

RSAConference2015

Singapore | 22-24 July | Marina Bay Sands



#RSAC

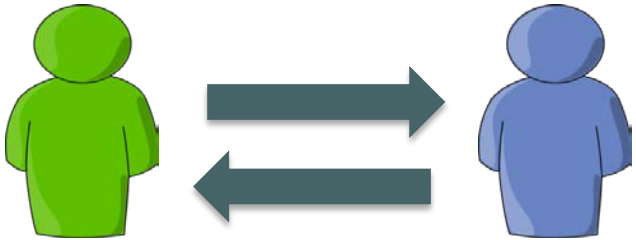
# Community Sharing

SPIRENT

# Community Sharing

## Typical Sharing Model

- Producers
  - Generate knowledge elements
  - Publish them onto the threat intelligence feed
- Consumers
  - Subscribe to the threat intelligence feed
  - Consume new knowledge elements as they are published



**Community members need to be both for Community Sharing to be successful**

# Community Sharing

- Disadvantages (Misconceptions)
  - Exposing attack data to potential threat actors
    - Someone with nefarious goals may be subscribed and now has access to data they didn't have before
  - Needing to sanitize data to protect yourself
    - Don't want to publish data about enterprise network infrastructure or application versioning
  - Time to publish new content to the community
    - Need to delay publishing the content until I have resolved all of my issues so I don't get re-hacked

SPIRENT

# Community Sharing

- Advantages
  - Sharing data means getting data
    - Some community driven feeds require participation to receive content
  - Expanding your knowledge base to include a larger dataset
    - Telemetry data outside your immediate dataset will help improve your overall threat modeling
  - Assisting others within your same industry vertical
    - Threat actors can (and sometimes do) stay within the same industry vertical
    - Learn about an attack before it reaches you!

**Knowledge is power!**

SPIRENT

RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

#RSAC

# Connecting The Dots…

SPIRENT

# Connecting The Dots…

**Use Case: Anthem BC/BS Data Breach (2014)**


- Insurance company that serves over forty million customers
  - 1 in 9 Americans according to Anthem's website
- Discovered breach January 29, 2014
  - Breach believed to have started weeks prior
- Expected costs over their $100M insurance Policy

- Data accessed / stolen included:
  - Names
  - Dates of birth
  - Social Security numbers
  - Health care ID numbers
  - Home addresses
  - Email addresses
  - Work information like income data

# Connecting The Dots…

**Use Case: Anthem BC/BS Data Breach (2014)**

- National Healthcare Information Sharing and Analysis Center (NH-ISAC)
  - Anthem, along with other major healthcare organizations, are members
  - Built the National Health Cybersecurity Intelligence System
    - Provides automated access, via STIX AND TAXII, to security intelligence and alert advisories

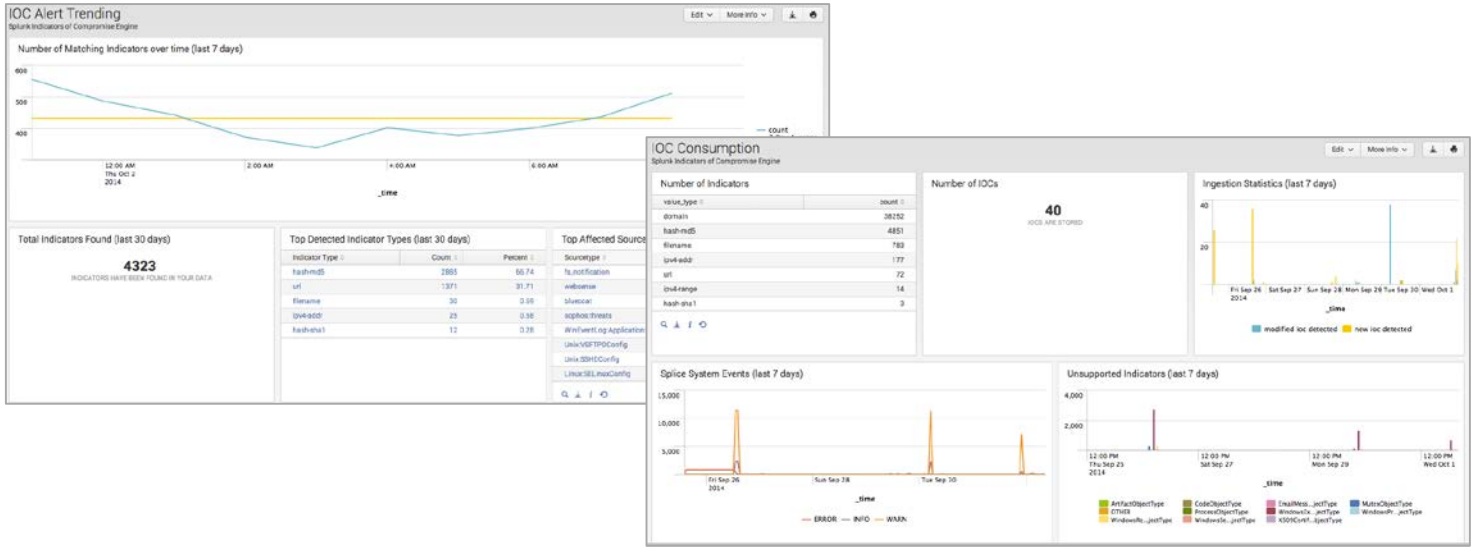
NH-ISAC

- Using community sharing, NH-ISAC was able to determine within 60 minutes the impact to its remaining members
- NH-ISAC also provided the IOCs to other ISACs within other verticals to measure larger cross-industry impact

SPIRENT

# Connecting The Dots…

- Leverage existing tools within your organization




**Splice App for Splunk**

# Apply What You Learned Today

- Next week
  - Identify weaknesses in your organization's security practices
  - Research included threat intelligence feeds or check within your organization's vertical
  - Look at internal software tools used today (i.e., SIEM) and see if any will incorporate threat intelligence feeds
- Within the next four weeks
  - Begin working with your own data to make it sharable knowledge elements
  - Incorporate at least one community driven threat intelligence feed into your threat modeling
- Over the next three months
  - Begin to contribute knowledge elements into the threat intelligence community
  - Build threat modeling for your organization off of proactive data driven by big data analysis

**Begin Threat Forecasting!**

RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

# Thank You!

#RSAC

SPIRENT

@david_desanto

https://www.linkedin.com/in/ddesanto