SANS

Cyber Threat Intelligence

SUMMIT & TRAINING

SANS360 SANS360

SANS DFIR

DIGITAL FORENSICS & INCIDENT RESPONSE

#CTISummit

Welcome! Welcome! Welcome!

- 9 Presentations
- 360 Seconds Each
- At 1 Minute Left – Warning
- At Bell –
  - Speaker Stops Speaking
  - Audience Erupts Into Applause
  - Next Speaker Takes Stage

#CTISummit

SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE

#CTISummit

SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE

Stephanie Scheuermann

- Cyber Threat Intelligence Specialist
- FORD MOTOR COMPANY

Go Further:
Create Intel Sharing Relationships

Foster and enrich cyber threat information sharing relationships, enhance existing trusted partnerships

Areas of Focus	Organizations
Top 5 IT partners	Select based on maturity of cyber security capability, value relationship has or will provide
Top 5-10 supplier /partners	Seek advice from business teams and legal on global suppliers of interest, also from incident data
Private sector companies in common vertical	Seek out confidentiality agreements with companies in common verticals
Internal business functions	Internal organizations with common business mission
Public sector	InfraGard Domestic Security Alliance Council (DSAC) Cyber Information Sharing & Collaboration Program (CISCP) **National Cyber Forensic Training Alliance (NCFTA)**

Business focused tactical and strategic actionable intelligence

Mike Green

- Sr. Manager Global Threat Intelligence
- DELOITTE

Recommendations

Document your organizations business objectives

Understand your organizations risk tolerance

Perform threat modeling and assess internal intelligence sources

Develop intelligence mindset / add data when you identify gaps

Develop internal researchers (Focused IoC's, Yara, CTI)

Mike Green
migreen@deloitte.com
610-479-5533

Deloitte.

Don McCoy

- Incident Response Manager
- ERNST & YOUNG

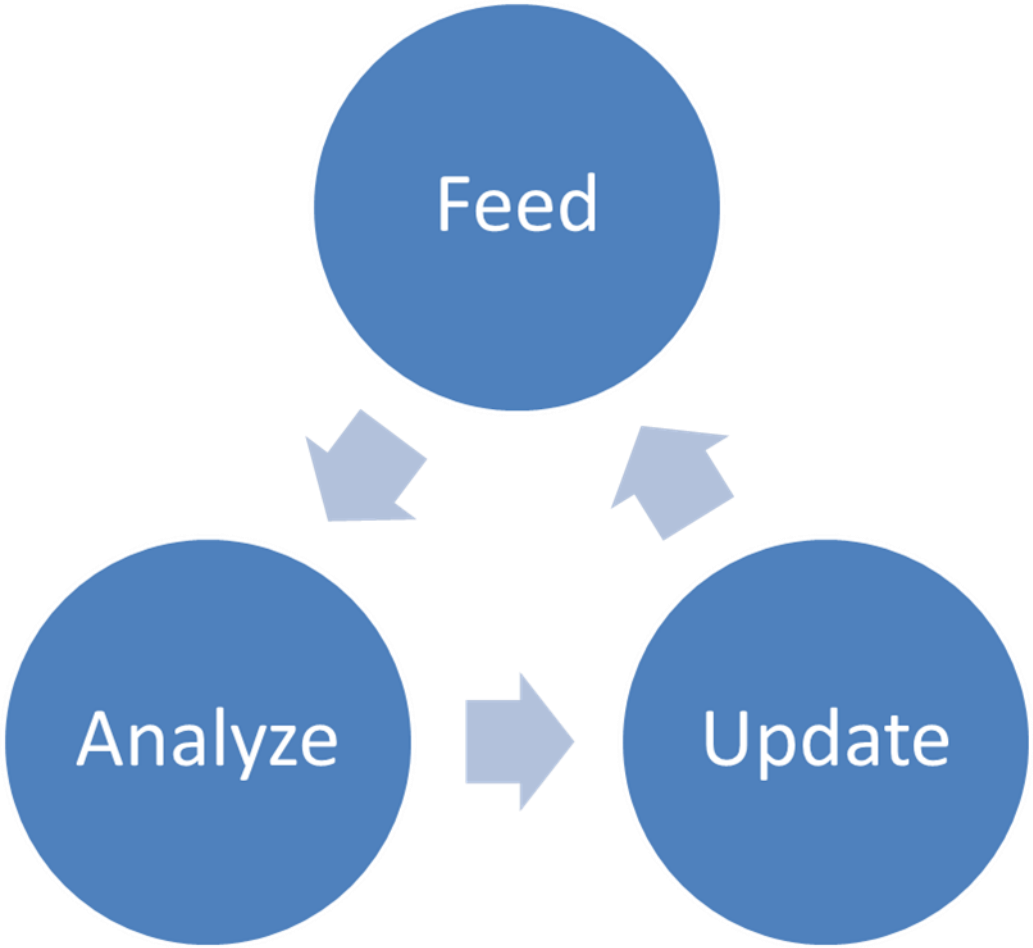
Developing Threat Intel With An Automated Analysis Framework

EY

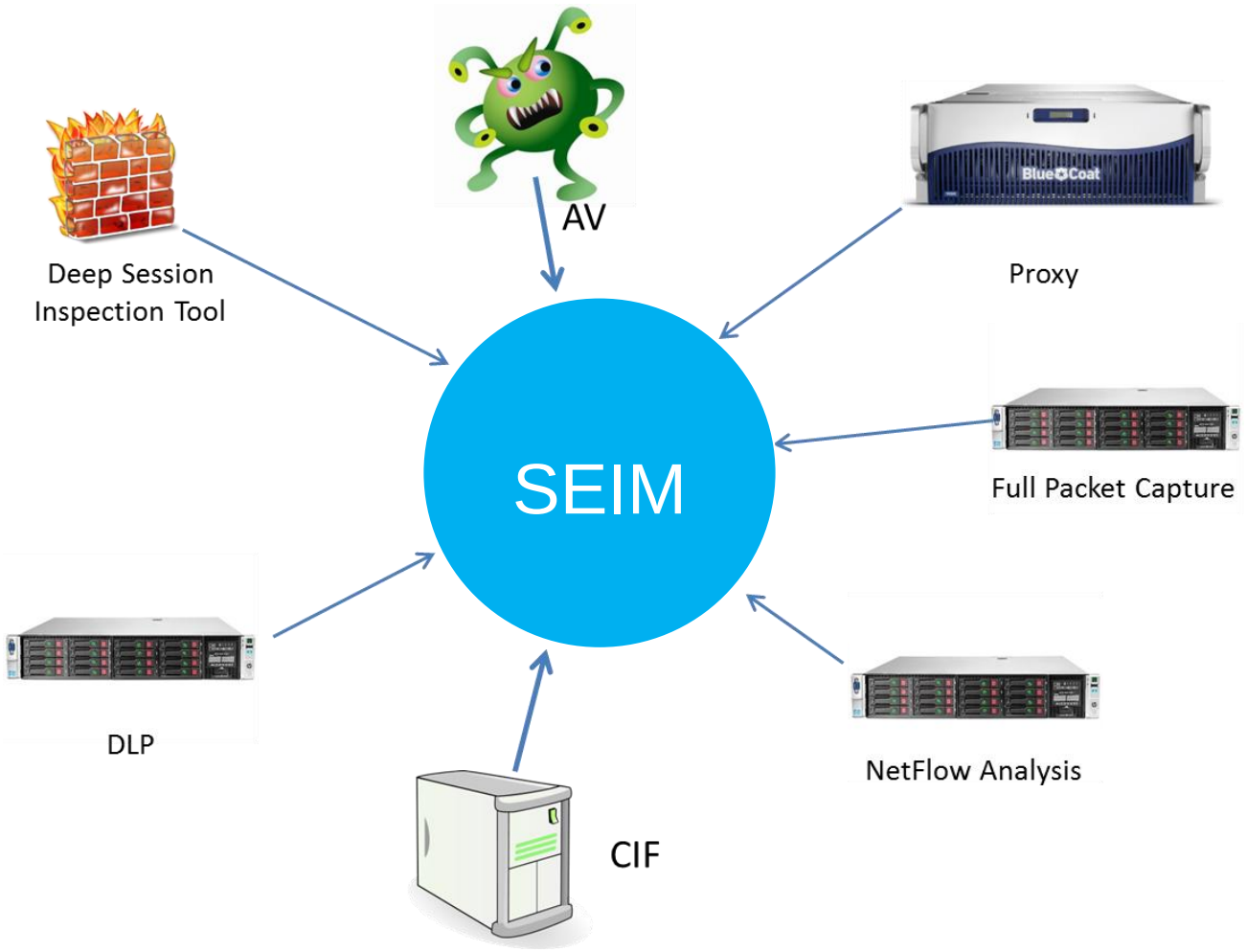
Building a better working world

Disclaimer Notice

Threat Intelligence Cycle



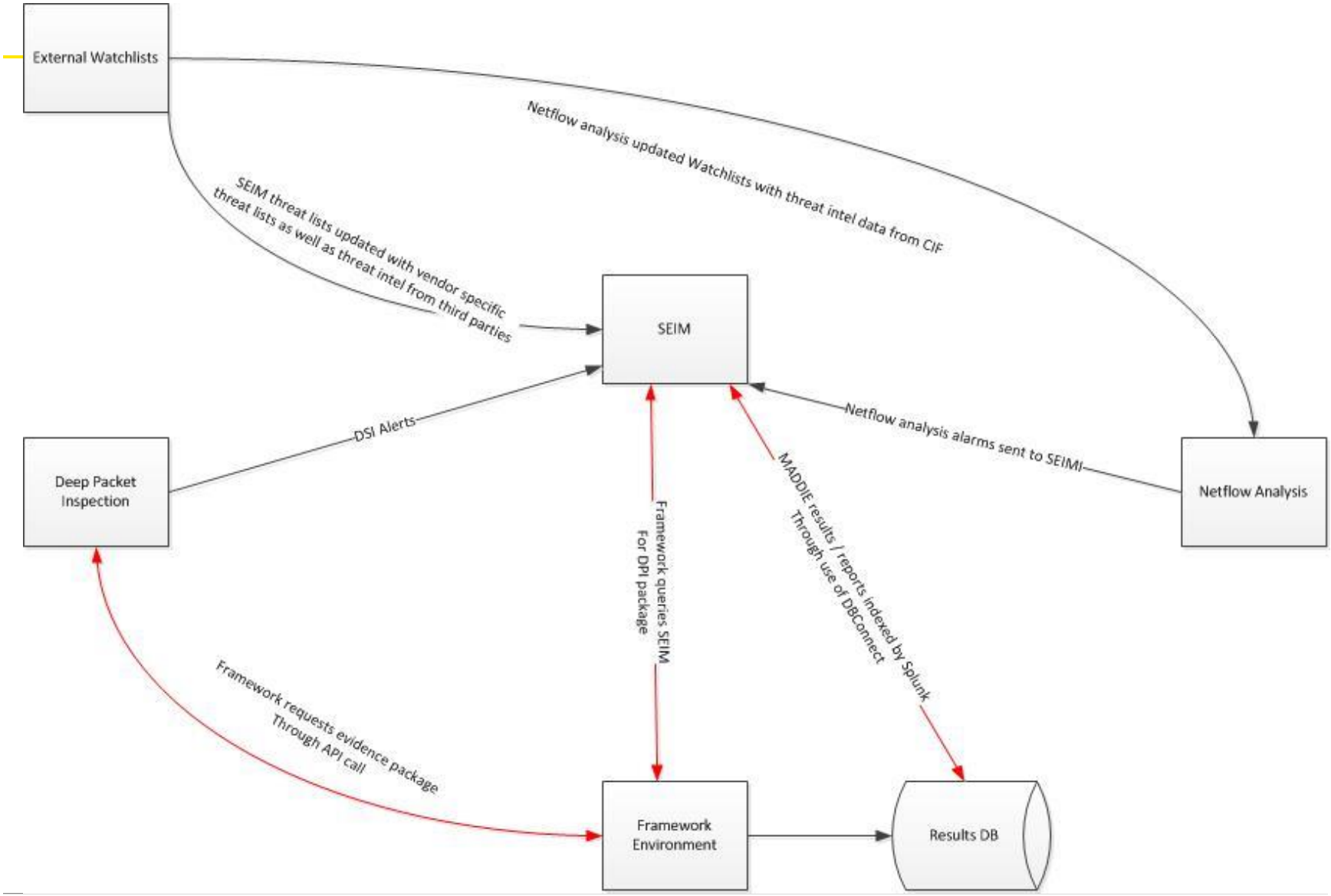
Ingesting Data



Analysis Framework

- Automated Framework designed for modularity
- Preprocessing intelligence to ensure sample is run only once
- Open source tools used for analysis
- Dumps relevant data to DB

How It All Fits Together



To Do

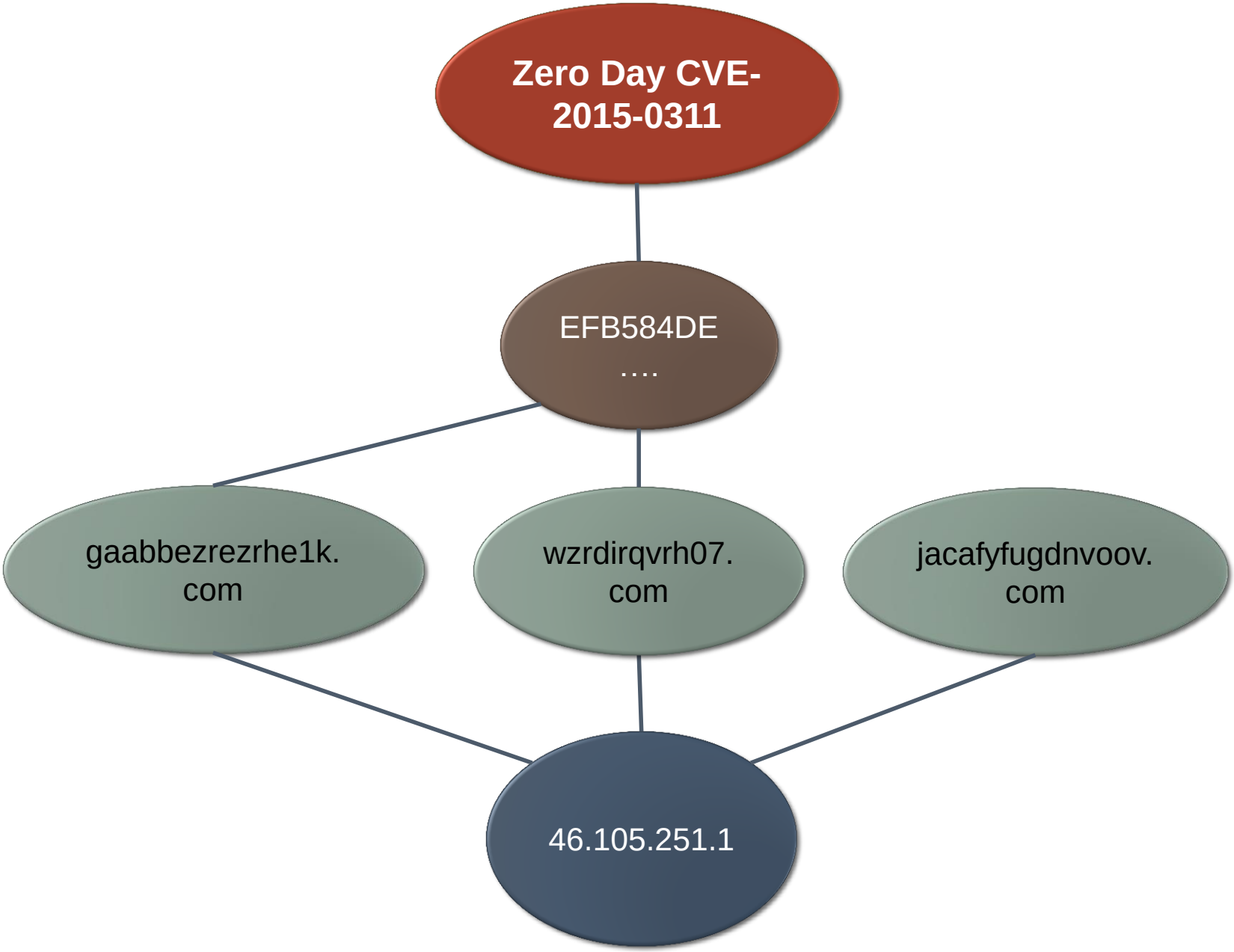
- Python Celery
  - Manage tasks sent to multiple MADDIE instances
- Integrate DLP policy violations
- Full Packet Capture alerts

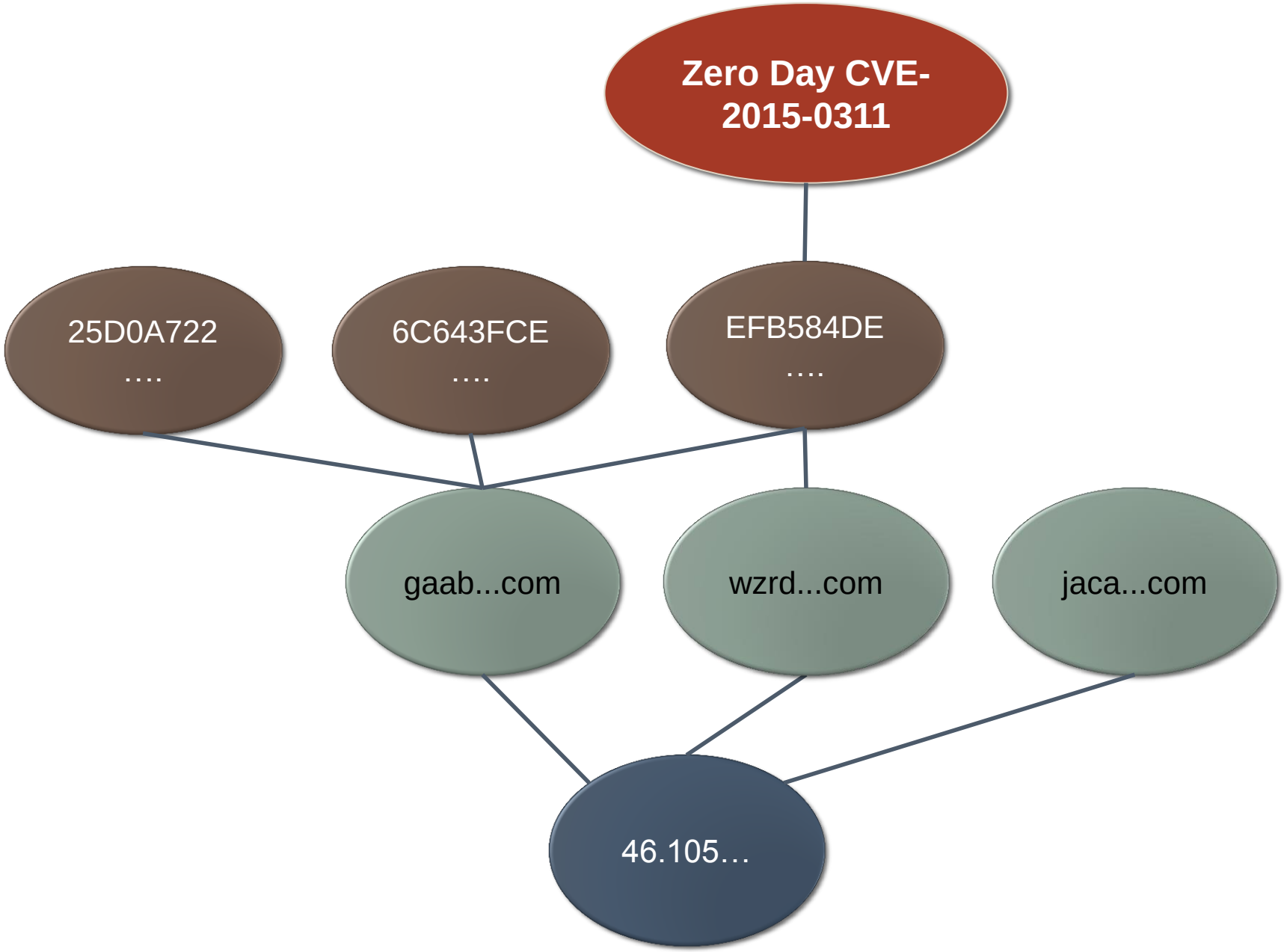
Roselle Safran

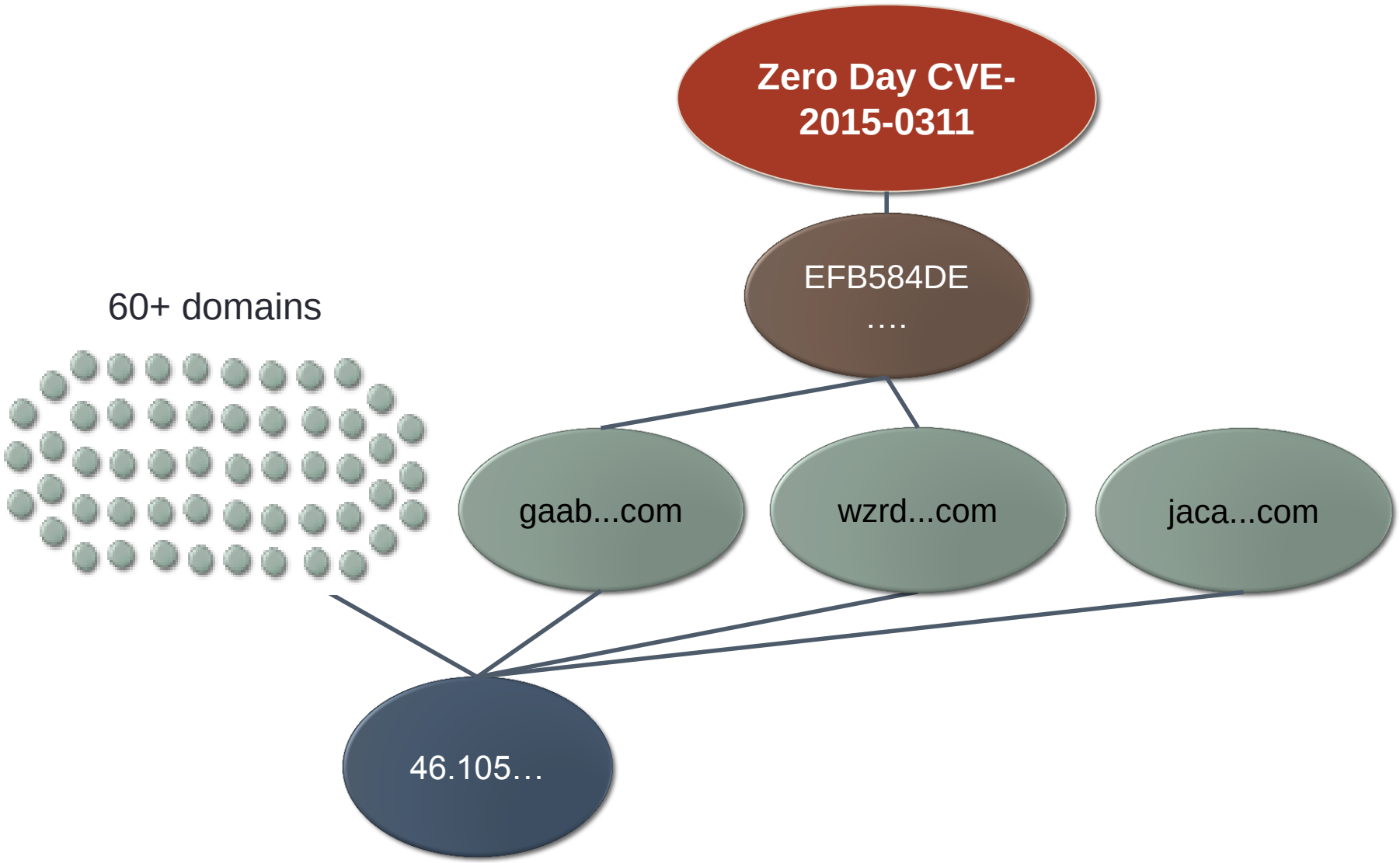
- Co-Founder/CEO
- UPLEVEL SECURITY

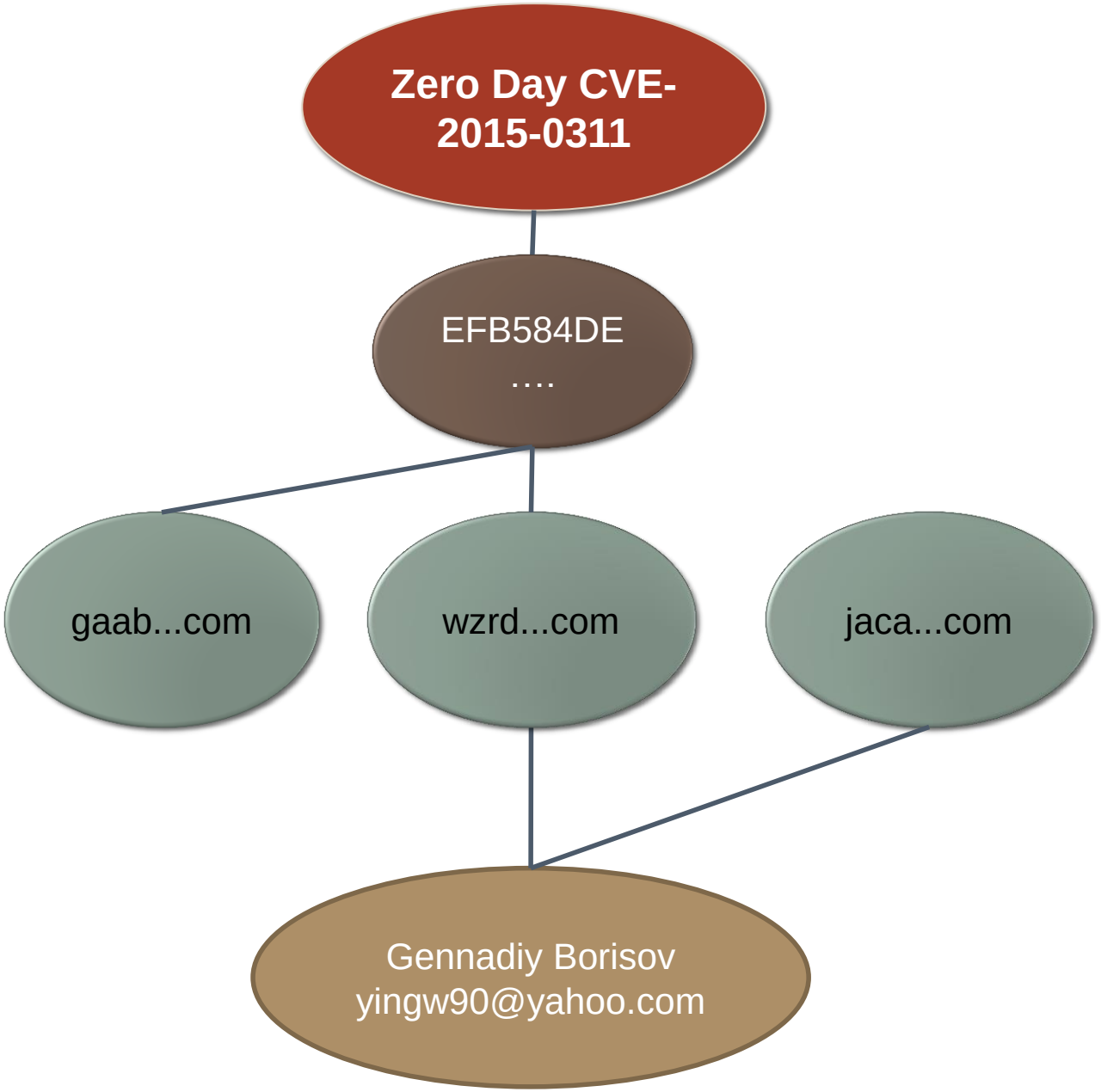
Connecting the Zero-Day Dots:
Using Data Visualizations of Open Source Intelligence to Uncover Attack Patterns

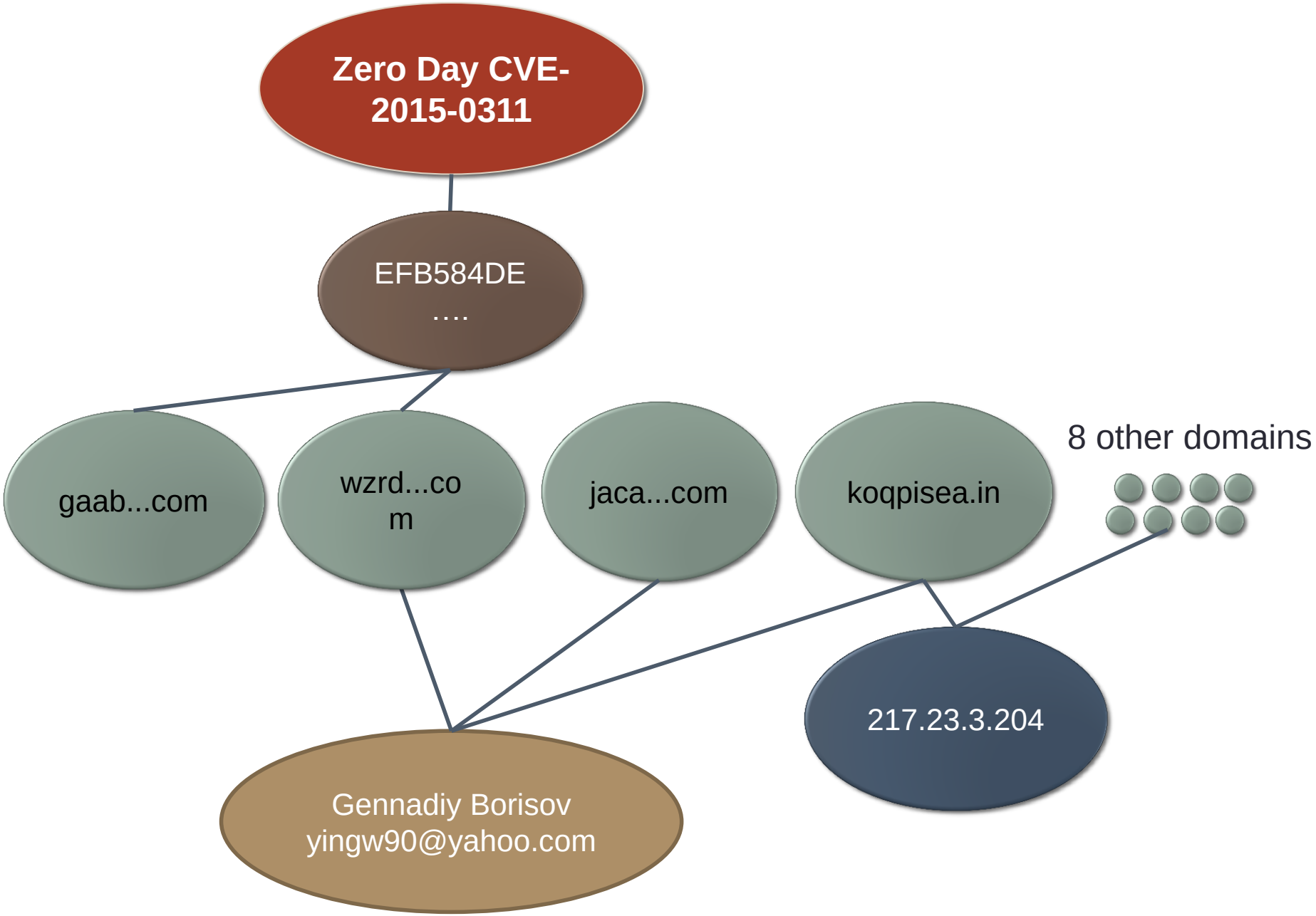
Roselle Safran
Uplevel Security

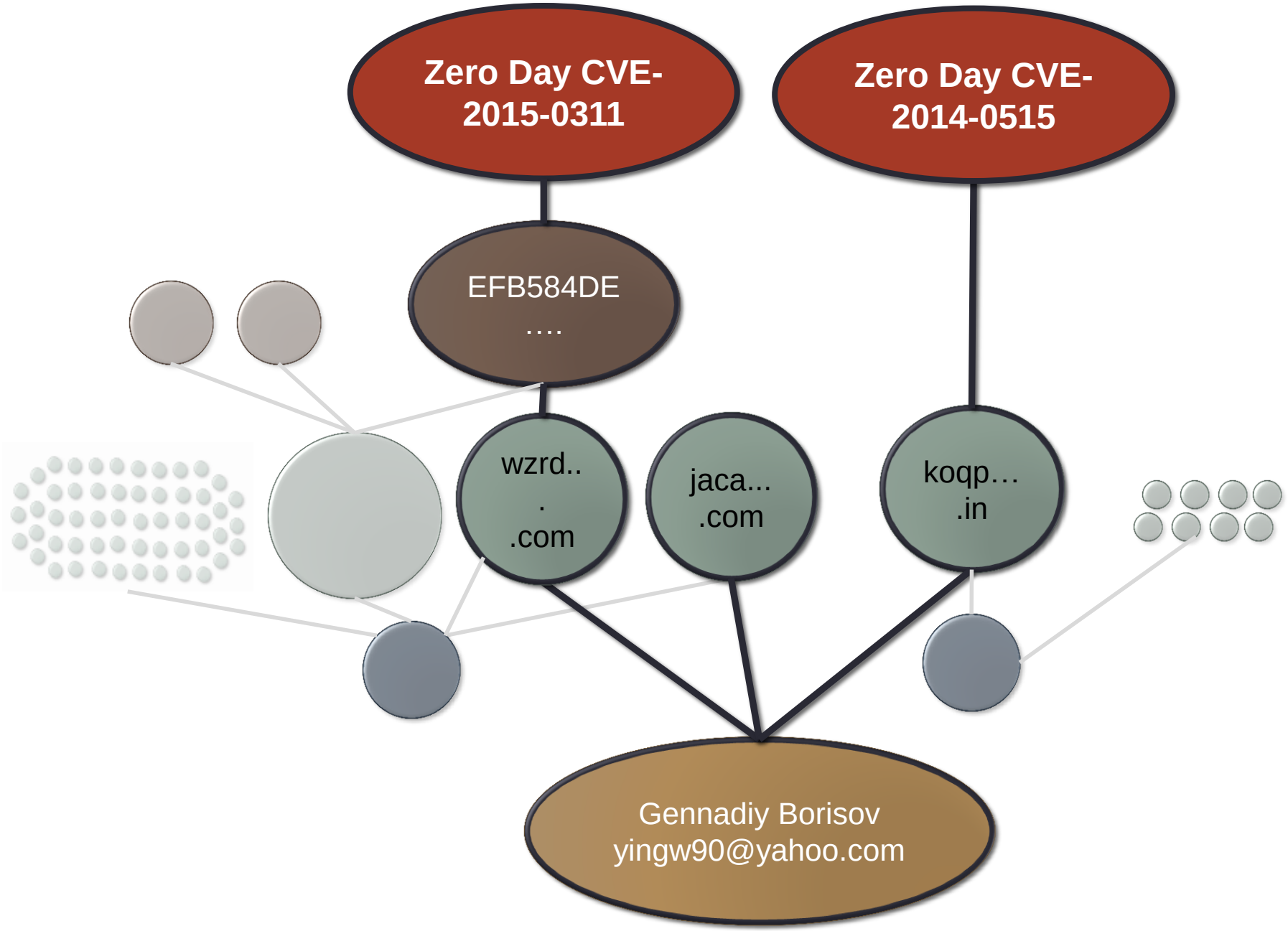

Zero Day CVE-2015-0311
EFB584DE ….
gaabbezrezrhe1k.com
wzrdirqvrh07.com
jacafyfugdnvoov.com
46.105.251.1


Zero Day CVE-2015-0311
25D0A722 ….
6C643FCE ….
EFB584DE ….
gaab...com
wzrd...com
jaca...com
46.105…


Zero Day CVE-2015-0311
EFB584DE
….
60+ domains
gaab...com
wzrd...com
jaca...com
46.105…


Zero Day CVE-2015-0311
EFB584DE
....
gaab...com
wzrd...com
jaca...com
Gennadiy Borisov
yingw90@yahoo.com


Zero Day CVE-2015-0311
EFB584DE ….
gaab...com
wzrd...com
jaca...com
koqpisea.in
8 other domains
217.23.3.204
Gennadiy Borisov
yingw90@yahoo.com


Zero Day CVE-2015-0311
Zero Day CVE-2014-0515
EFB584DE
….
wzrd..
.
.com
jaca...
.com
koqp…
.in
Gennadiy Borisov
yingw90@yahoo.com

Thank you!

roselle@uplevelsecurity.com

Dominique Kilman

- Manager
- KPMG, LLP

KPMG

Threat Intel
Let's do this!

Dominique Kilman
Matt Bromiley

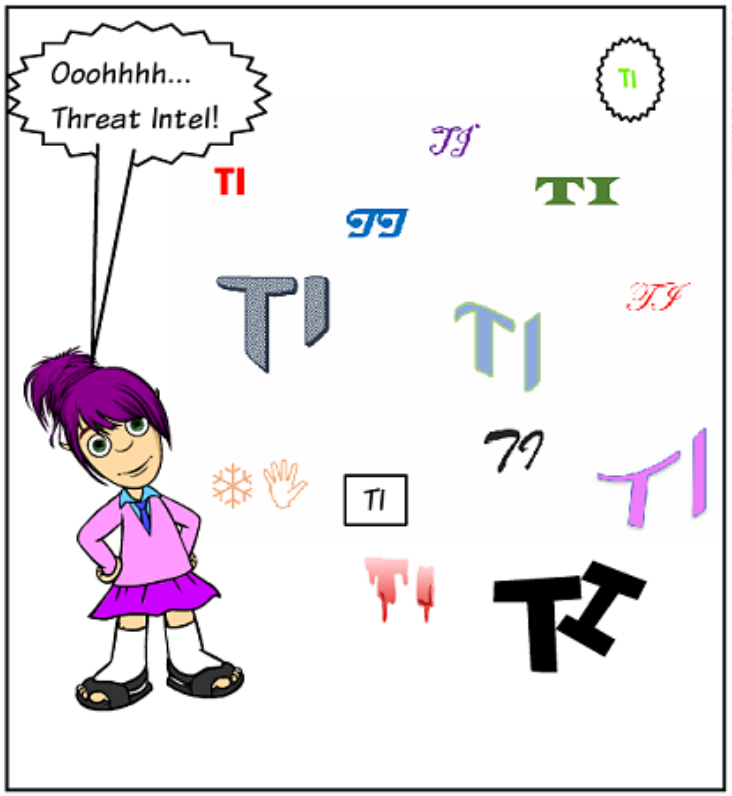
Meet the heroes of our story…

Current State

There must be a better way….

A secure network… wrapped up with a bow!

(Pink, of course)



Everyone's talking about it… it must be good.

There's even a SANS summit dedicated to it!

Add in all that intel…

Add some fairy dust

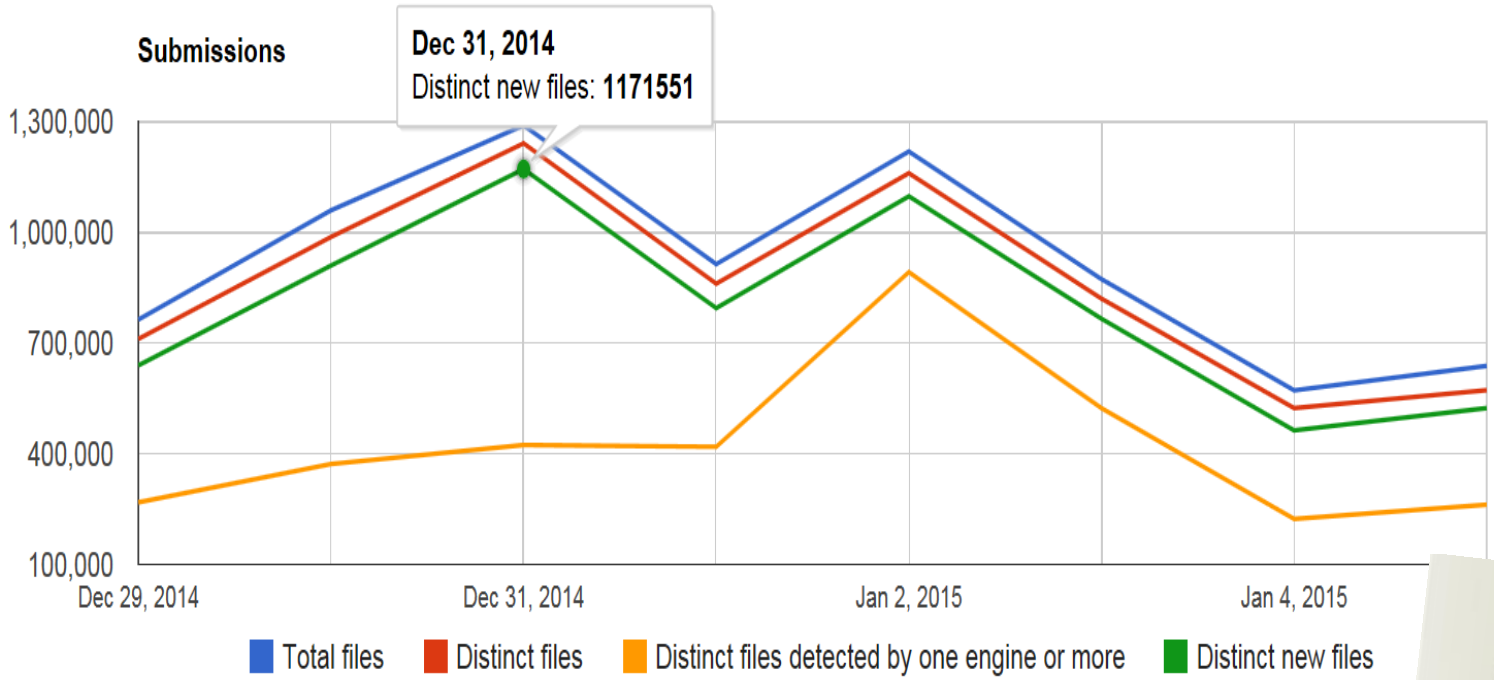
mix vigorously


Everything's se
All the intel....
uhhmm...DK?!?
Security
ZZZ
ZZZZZ
ZZZZZZ
WWW.TOONDOO.CO

Well… that didn't work out as expected!

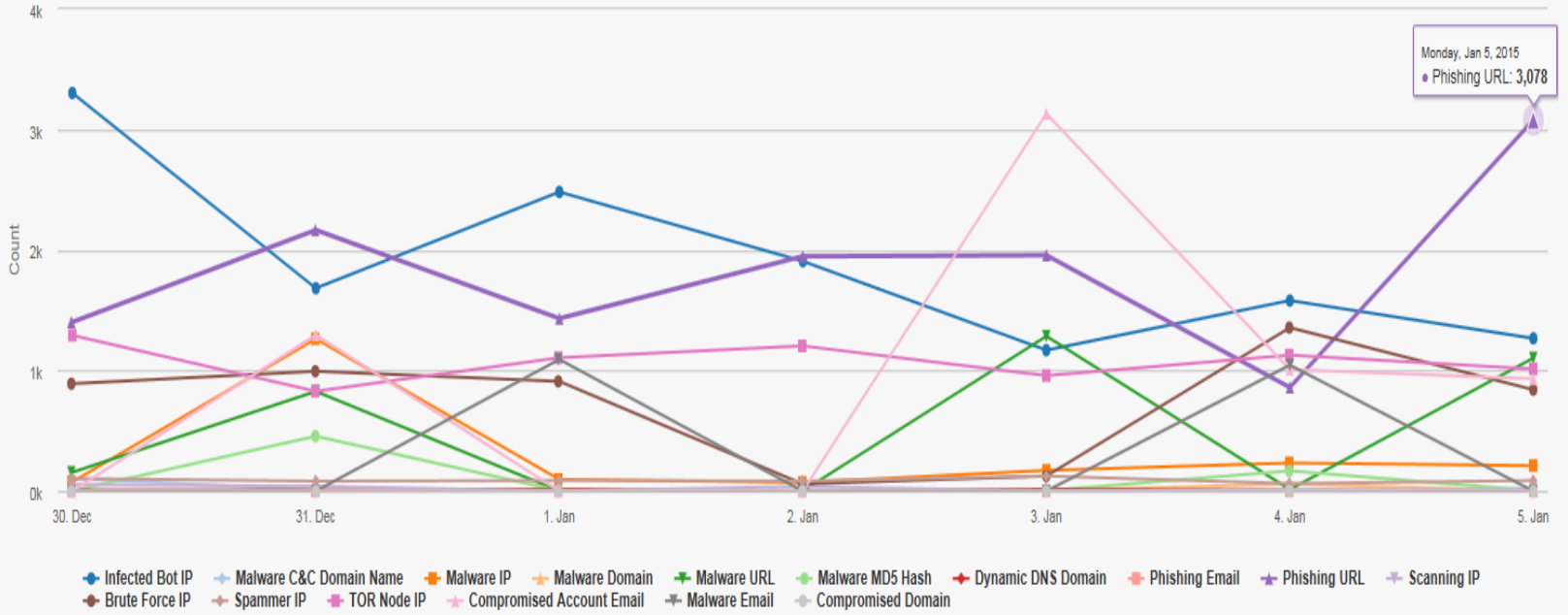
What happened?

virustotal


Submissions
Dec 31, 2014
Distinct new files: 1171551
1,300,000
1,000,000
700,000
400,000
100,000
Dec 29, 2014
Dec 31, 2014
Jan 2, 2015
Jan 4, 2015
Total files
Distinct files
Distinct files detected by one engine or more
Distinct new files

THREATSTREAM

Weekly Stats




But isn't more information better?
Not really. Lets see what happened when an organization turned on default threat rules in their alert system
WWW.TOONDOO.COM

Alert Review

Urgency

CRITICAL	0
HIGH	0
MEDIUM	0
LOW	4151
INFO	0

Owner: All

Name:

Security Domain: All

Search: Threat - Threat List Activity - Rule

Time: from Dec 19 throug...

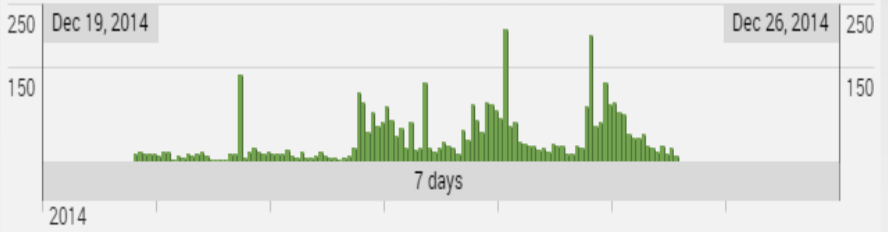
Status: × ALL

Submit

Job | Smart Mode

✓ 4,151 events (12/19/14 12:00:00.000 AM to 12/26/14 12:00:00.000 AM)

Format Timeline | – Zoom Out | + Zoom to Selection | × Deselect | 1 hour per column



Edit all selected |

« prev 1 2 3 4 5 6 7 8 9 10 next »

i		Time	Security Domain	Title	Urgency	Status	Owner	Actions
›	☐	12/24/14 1:11:15.000 PM	Threat	Threat List Activity Detected (bidder-us-west-2.tlvmedia.com)	Low	New	unassigned	⌄
›	☐	12/24/14 1:11:15.000 PM	Threat	Threat List Activity Detected (101.199.103.183)	Low	New	unassigned	⌄
›	☐	12/24/14 1:11:15.000 PM	Threat	Threat List Activity Detected (101.199.103.181)	Low	New	unassigned	⌄
›	☐	12/24/14 1:11:15.000 PM	Threat	Threat List Activity Detected (api.boxrock.info)	Low	New	unassigned	⌄
›	☐	12/24/14 1:11:15.000 PM	Threat	Threat List Activity Detected (61.160.224.190)	Low	New	unassigned	⌄

12/24/14 1:11:15.000 PM	Threat	Threat List Activity Detected (bidder-us-wes

Description:

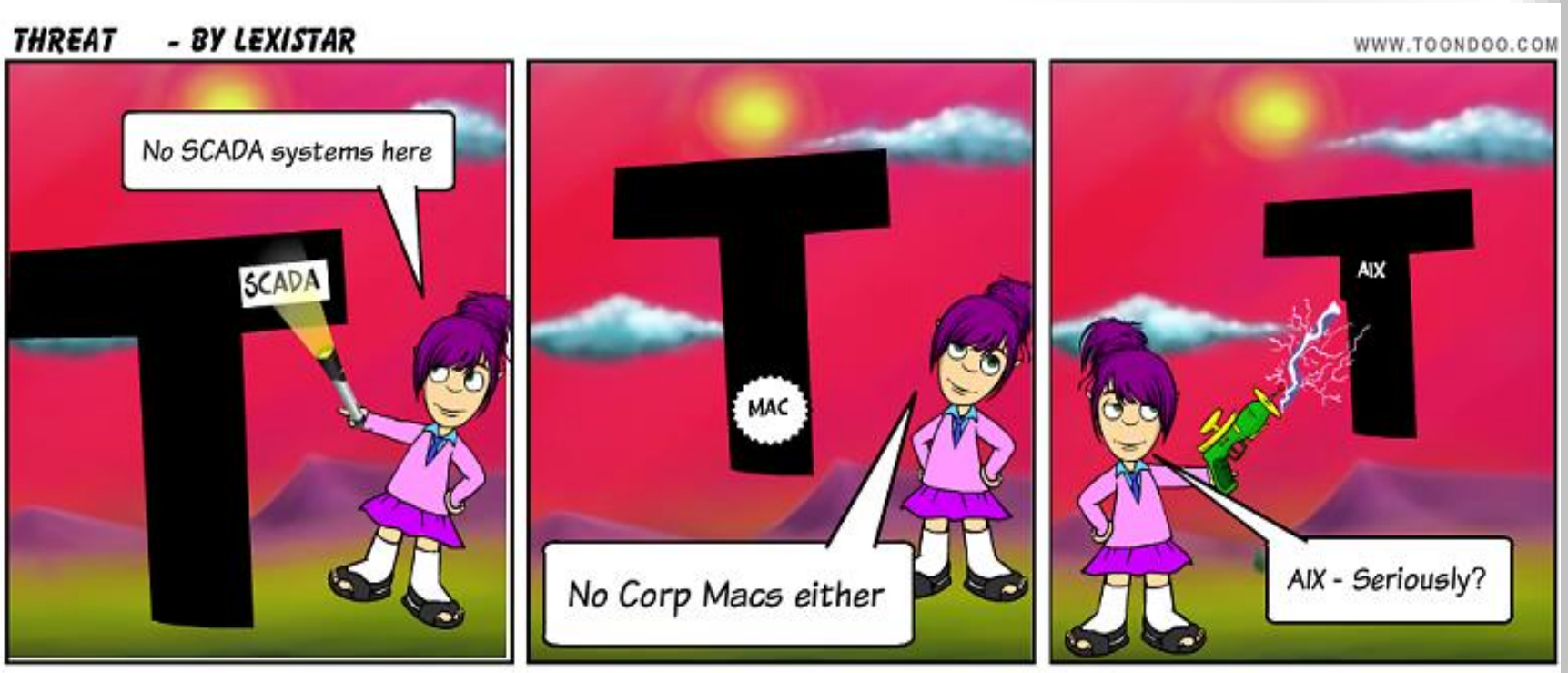
bluecoat_v5 network communication was discovered involving a server listed on one or more threat lists (bidder-us-west-2.[redacted].com).

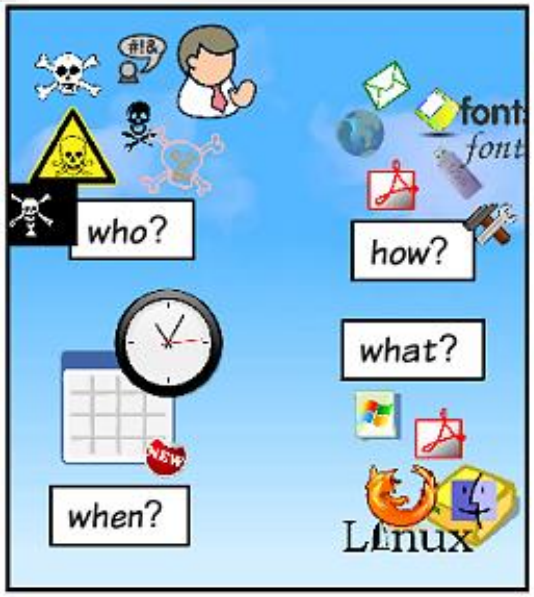
Additional Fields	Value	Action
Destination	bidder-us-west-2.t[redacted]com	
Destination Expected	false	
Destination PCI Domain	untrust	
Destination Requires Antivirus	false	
Destination Should Time Synchronize	false	
Destination Should Update	false	
Destination Threat List Description	malware (xref: blog[redacted]com)	
Destination Threat List Name	malware_domains	
Source	10.58.95.11	
Source Expected	false	
Source PCI Domain	untrust	
Source Requires Antivirus	false	
Source Should Time Synchronize	false	
Source Should Update	false	
URL	unknown	

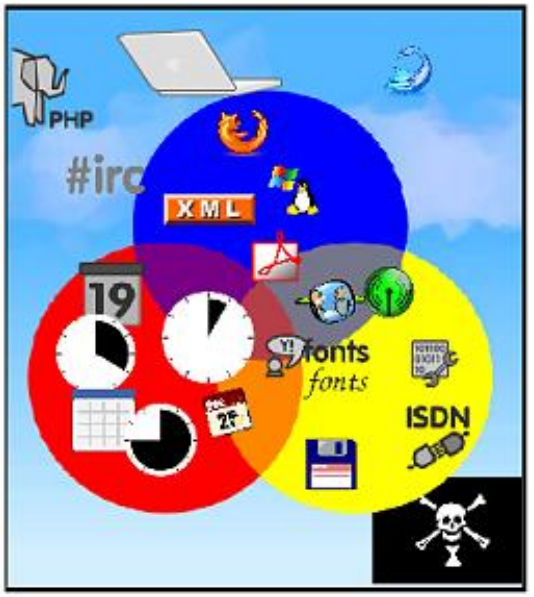
Event Details:


We need to put the "Intelligence" into threat INTEL
And while we're at it - lets scope the threat in THREAT intel!
Let's DO this!

What is YOUR threat… really…







Is there any intelligence in that "intel?"

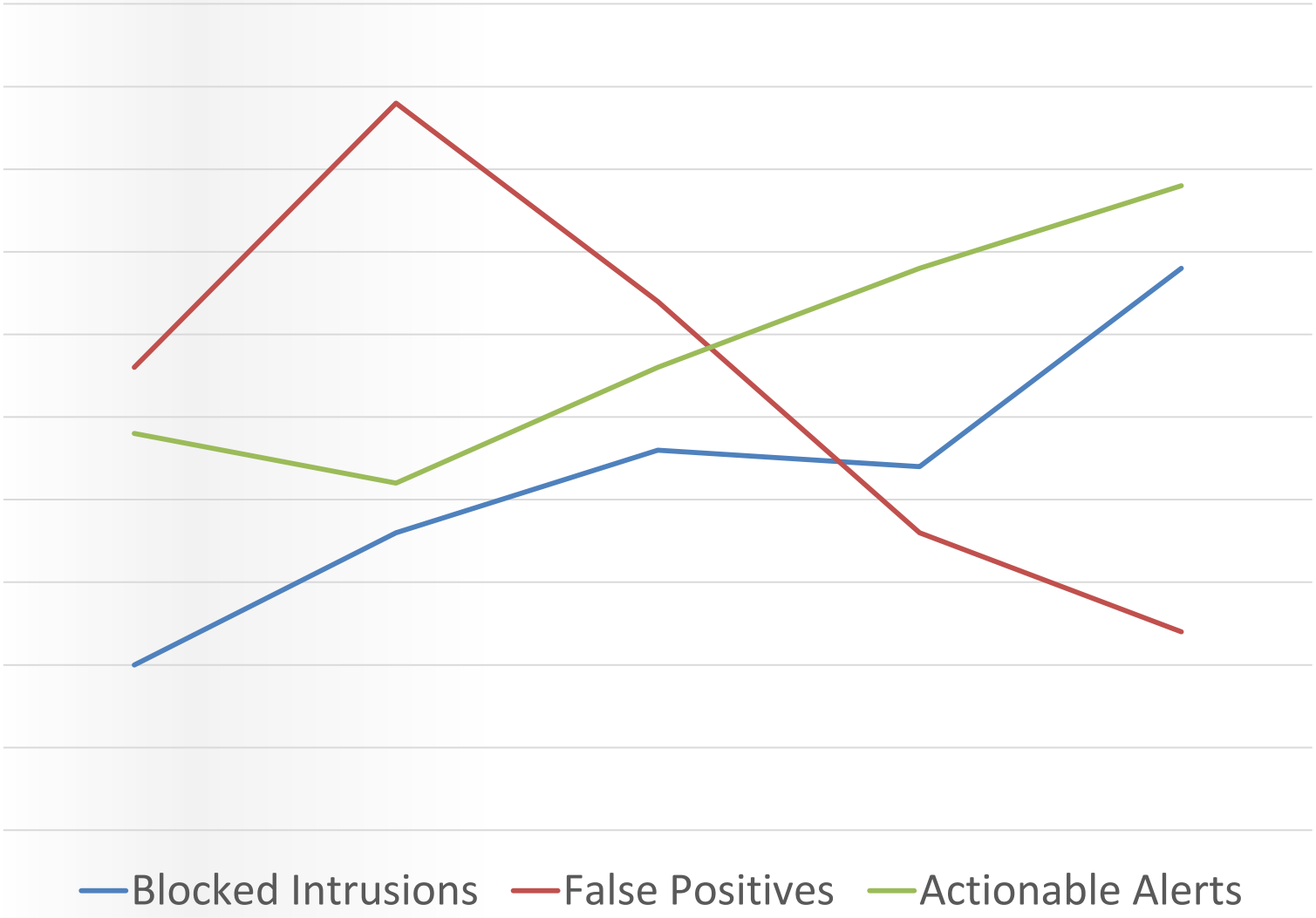
- Who
- What
- When
- How
- How long
- How do you know
- Do you care

Add TI

Tune

Monitor &
Test

Security Program Metrics

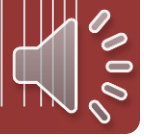


The

Matt Bromiley
@505Forensics

End

Dominique Kilman
@dominique_97



Michael Lotas

- Chief Cyber Security Architect
- GENERAL DYNAMICS FIDELIS

Ray Strubinger

- Security Event Response Team Lead
- ERNST AND YOUNG

Operationalizing Self Sourced Threat Intel

Ray Strubinger, SERT Lead

February 2015

Building a better working world

Standard Disclaimer

Background & Definitions

- What to we mean by “self-sourced” intel?
- How does self-sourced intel differ from external threat sources?

Response Options

- No matter the source of the intel there are three general response options
  - Immediate mitigation
    - Block - Networks, IP addresses, or file hashes
  - Research, Prioritize & Respond
    - Understand potential business impact
    - Determine the scope and history
      - Has this activity or these indicators been seen previously?
    - Take action now or wait?
  - No action

Preparing for Action

- Gain an understanding of the environment
  - Logs
    - Format, volume, velocity, location, and contents
  - Network
    - Routers, firewalls and other security systems
- Develop a capability to review logs
  - Numerous commercial & open source options
  - Indicators may be found here

Taking Action

- Combine log data and intel
  - Determine the scope
    - Tip of the iceberg or a flash in the pan?
    - Initiate a formal response?
- Identify patterns
  - Are there commonalities among the indicators or in the logs?
  - Patterns can be used to develop broader strategy
  - Initiate a formal response?
- Retiring intel
  - Keeping indicators fresh

Questions?

Joshua Ray

- Director, Cyber Security Intelligence
- VERISIGN iDEFENSE

VERISIGN

Six Approaches to Creating an Enterprise Cyber Intelligence Program

Josh Ray, Senior Director & GM Verisign iDefense

6 Approaches to build a Cyber Intel Program

powered by

VERISIGN™

Rob Lee

- DFIR Lead
- SANS Institute

CYBER THREAT INTELLIGENCE #FAILS

SANS DFIR

DIGITAL FORENSICS & INCIDENT RESPONSE

“CTI” is the new “APT”

THREAT

“One Down. Billion to Go.”

SECTEC ASTRONOMY

Captain Obvious

- Thank you for attending!

- Please fill out speaker evaluations on your way out.