IID

27th ANNUAL FIRST CONFERENCE

BERLIN

14-19 JUNE 2015

UNIFIED SECURITY: IMPROVING THE FUTURE

Presented by Rod Rasmussen

June 16, 2015 FIRST Conference, Berlin

IID

Quality Over Quantity

CUTTING THROUGH CYBERTHREAT INTELLIGENCE NOISE

Rod Rasmussen

IID founder, CTO

Co-chair Anti-Phishing Working Group’s Internet Policy Committee

Member of:

ICANN's Security and Stability Advisory Committee

Online Trust Alliance’s Steering Committee

FCC Communications Security, Reliability and Interoperability Council

Messaging Malware Mobile Anti-Abuse Working Group

Forum of Incident Response and Security Teams (FIRST Representative)

DNS-OARC

MBA from Haas School of Business UC-Berkeley; bachelor's degrees in Economics and Computer Science from University of Rochester

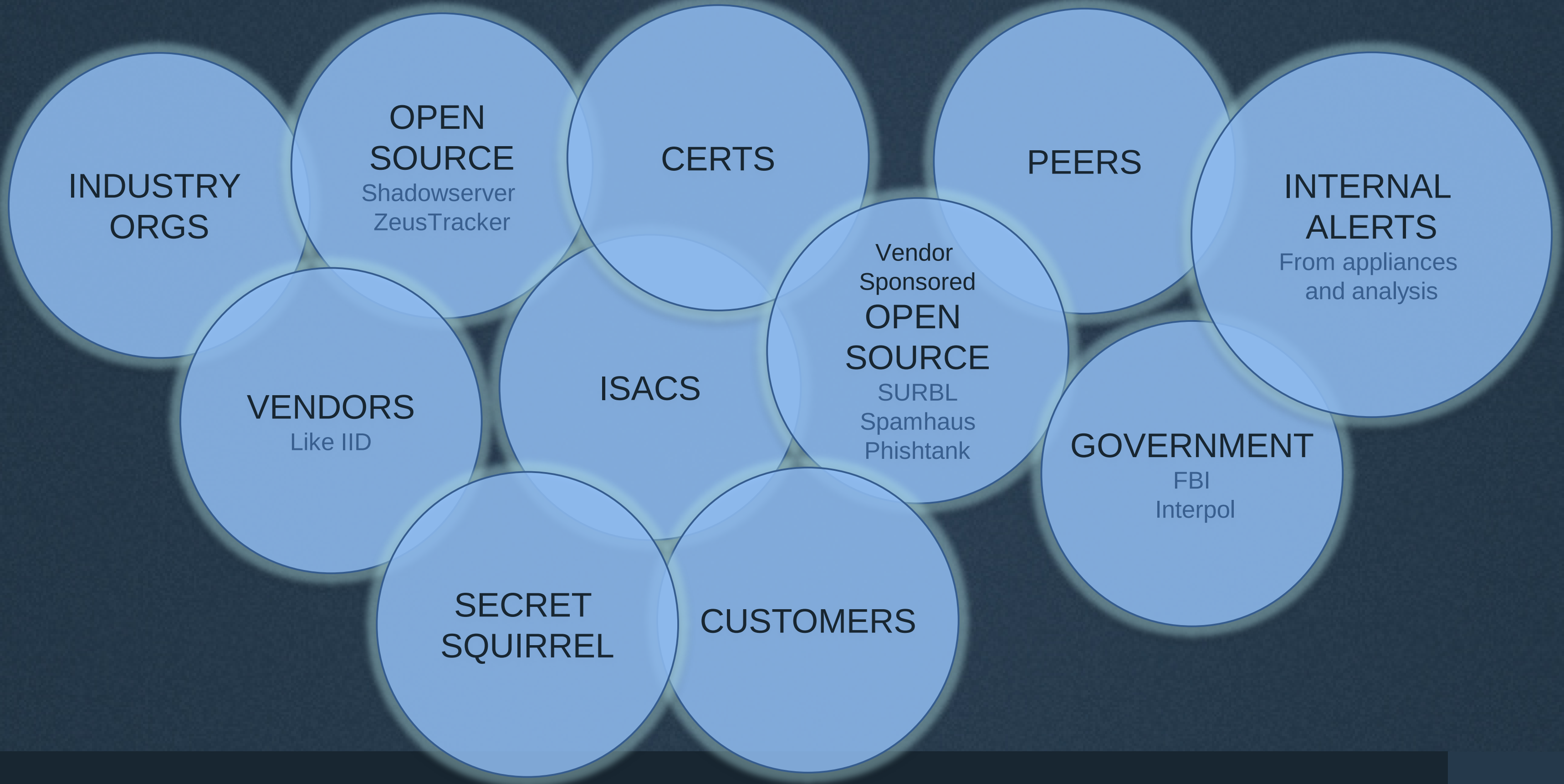
Cutting through cyberthreat intel noise

- Threat intel source overload
- How to cut out noise
- Threat intel plug and play with security appliance

Problem

- Over 90% of data breaches in 1H 2014 could have been avoided with simple controls and best practices
- Security controls and best practices are valuable but only you have the right threat intelligence
- How to choose data from thousands of threat intelligence sources

Threat intel source overload



INDUSTRY ORGS

OPEN SOURCE
Shadowserver
ZeusTracker

CERTS

PEERS

INTERNAL ALERTS
From appliances and analysis

VENDORS
Like IID

ISACS

Vendor Sponsored OPEN SOURCE
SURBL
Spamhaus
Phishtank

GOVERNMENT
FBI
Interpol

SECRET SQUIRREL

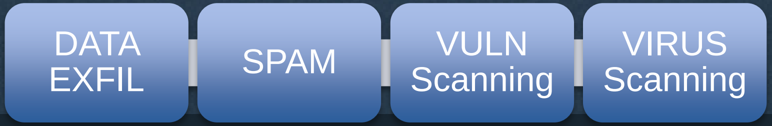
CUSTOMERS

All intel is useful for something—use case matters most!

- Life is shades of gray, not black and white
- Reputation and context are key for use
- Block | Alert | Inform scoring | “Fits a pattern”
- For example, google.com

  In an ISP blacklist = disaster.

  In a malware analysis tool doing wireshark on
  a bare-metal honeypot = sign of malware activity
- Fit the data to your purpose



DATA EXFIL

SPAM

VULN Scanning

VIRUS Scanning

Dangers of threat intel that’s just noise

- False positives
- Incomplete or missing context
- No concept of TTL or useful life
- Lack of understanding good applications for data

Noiseworthy vs. noise

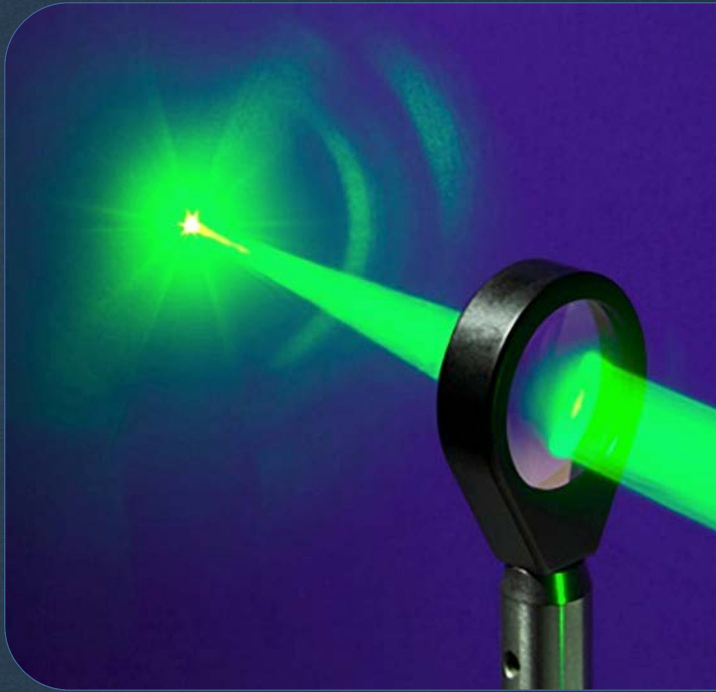
Determine trustworthiness of source

Use internal threat intel and reputation to determine false positives

Analyze metrics across all data

Increase confidence with correlation, frequency and source reputation

Expand context by linking related data points to previous unknowns



Machine to machine delivery

- With your game plan set, how to get data into security appliances and analysis tools
- Scale is key–attacks are ubiquitous
- Hub and spoke vs. peer to peer
- Correlation, analysis, prioritization
- Feedback loops

Um, that’s a lot of data…

- Appliances can only handle so much data
- Prioritize based on problem you’re solving and implementation ease
- Refresh rates
  - Performance
  - Timeliness
  - Cost/bandwidth

You still need manual data in production

- Translating a research project or buddy’s email into network protection

- Inventory how you do (or wish you did) things today

- Automating a bunch of manual processes

Choose the right security appliances

- SIEM
- Next Gen Firewall
- IDS/IPS
- Web Proxy
- DNS Server
- Email Filter
- Internal TI Repository
- Research Tool
- Log Analysis
- Advanced Threat Detection

Choose the
right data format

STIX	NMSG
CSV	IODEF
JSON	XLS
XML	CEF
Open IOC	

Working with various formats

Battle plan: format that delivers for the given use case

The right tools to translate

Push through repositories or services to normalize

Questions

IID

Rod Rasmussen, President & CTO
rod.rasmussen <at> internetidentity.com