

SANS 2022 Cyber Threat Intelligence Survey

Today's Speakers

- **Pasquale Stirparo**, *SANS Certified Instructor Candidate & SANS CTI Survey Author*
- **Rebekah Brown**, *SANS Certified Instructor Candidate & SANS CTI Survey Author*
- **Megan Gooch**, *Manager Threat Research, EclecticIQ*
- **Bob Hansmann**, *Sr. Product Marketing Manager, Infoblox*
- **David Monnier**, *SANS Fellow, Team Cymru*

Today's Agenda

- SANS 2022 CTI Survey: Key Findings and Trends—Rebekah Brown
- Observations on Responses from the 2022 SANS CTI Survey—Megan Gooch
- Demonstrating CTI Value Through Defense, Investigation, and Response—Bob Hansmann
- How Pure Signal Recon Gives You an Advantage—David Monnier
- Panel Discussion—Pasquale Stirparo, Megan Gooch, Bob Hansmann, David Monnier



Join the SANS Analyst Program Slack Workspace

<http://sansurl.com/analyst-research-content>

#00-help – Having technical difficulties? Let us know here, we're ready to help!

#discussion – Chat with our SANS authors, sponsor speakers, and fellow attendees to discuss presentations and post questions!

You can also connect directly with sponsor speakers on their own channels:

- **#sponsor-eclecticiq**
- **#sponsor-infoblox**
- **#sponsor-team-cymru**

Code of Conduct

SANS strives to create an atmosphere of learning, growth, and community. We value the participation and input, in this event and in the industry, of people of all genders, sexual identities, cultural and socioeconomic backgrounds, races, ethnicities, nationalities, religions, and ages.

Please support this atmosphere with respectful behavior and speech. This applies to all online interactions including the event Slack channel and in Zoom.

**If you witness or experience anything contrary to these guidelines, please tell us at:
analyst@sans.org**



Questions or Comments?

Connect with Pasquale Stirparo, SANS

For General Event Discussion:
#discussion



Questions or Comments?

Connect with Rebekah Brown, SANS

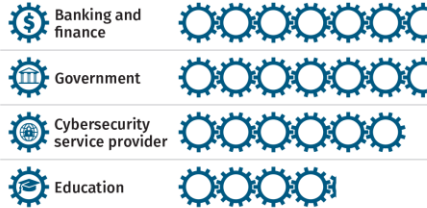
For General Event Discussion:
#discussion

Key Takeaways

- Increase in organizations just building out their CTI capabilities
- Continued downward trend in collaboration between CTI teams and other stakeholders
- CTI teams still struggle with measuring impact
- Many teams are not using consolidated threat intelligence platforms, and many use home-built tools

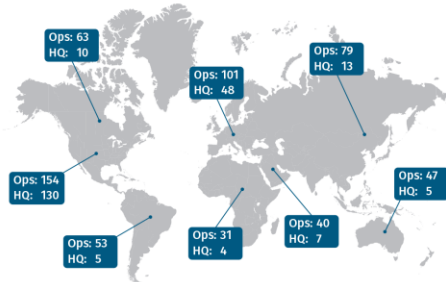
CTI Team and Processes

Top 4 Industries Represented

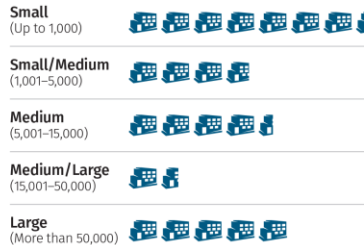


Each gear represents 5 respondents.

Operations and Headquarters



Organizational Size



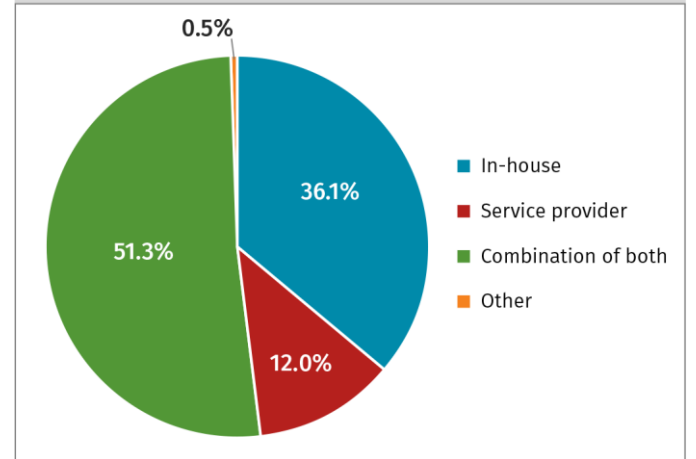
Each building represents 10 respondents.

Top 4 Roles Represented



Each person represents 5 respondents.

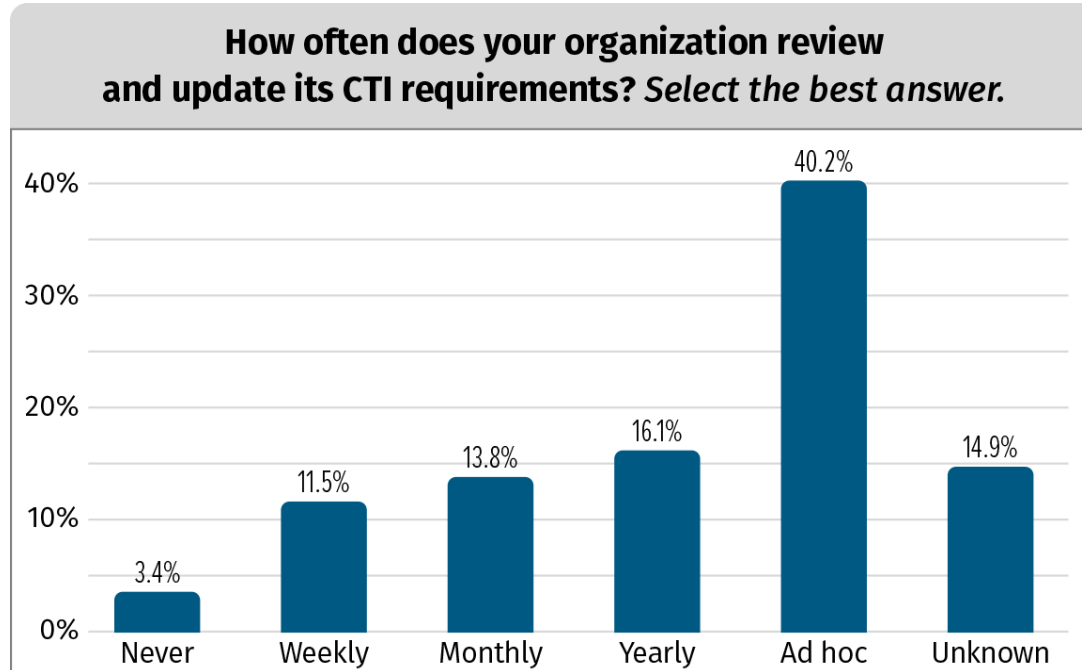
Are your CTI functions and activities handled in-house, by a service provider, or through a combination of the two?



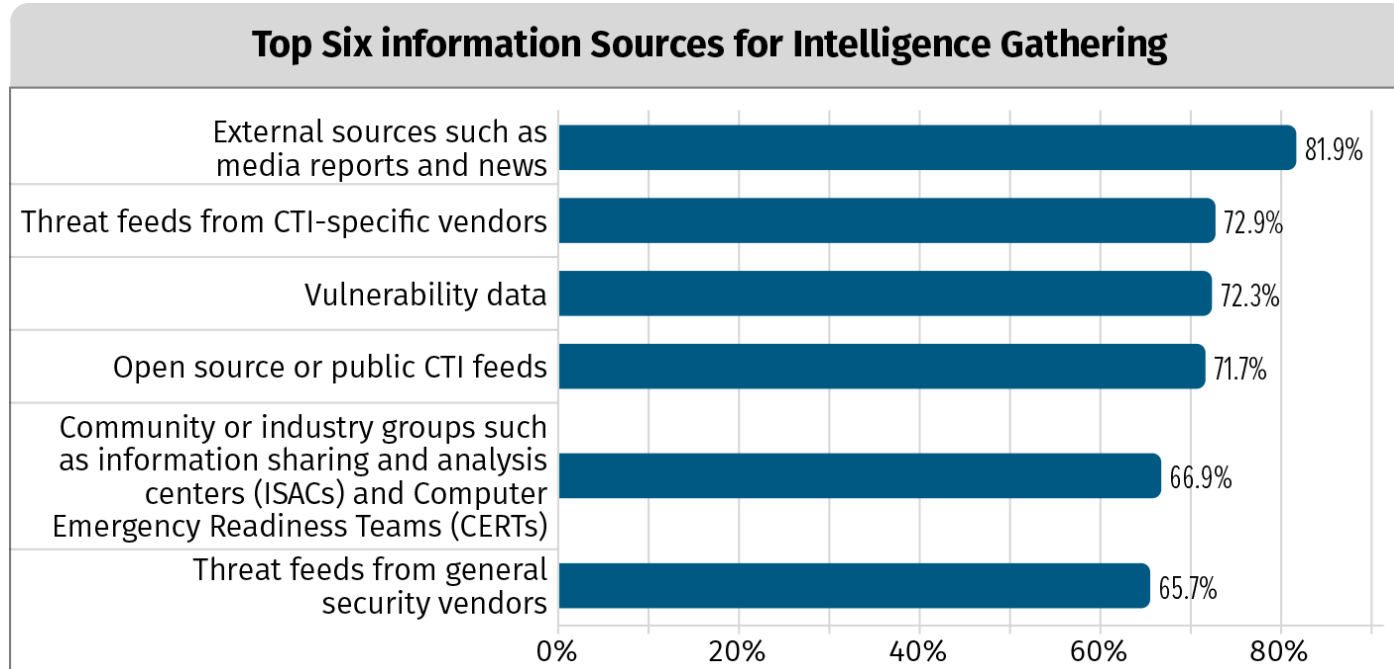
Uses for CTI

- Most useful forms of CTI at present:
 - Detailed information about malware
 - Information about vulnerabilities being leveraged
 - Broad attacker trends
- Most useful in the next 12 months:
 - Industry-specific attack information
 - True attribution of adversaries

Requirements



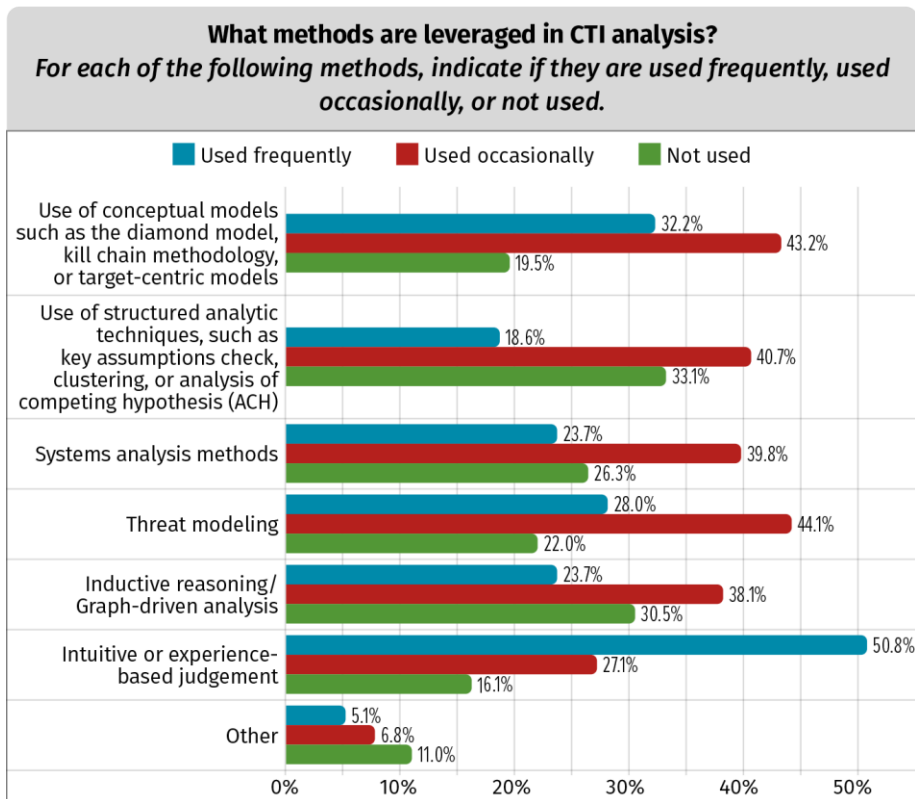
Collection Sources



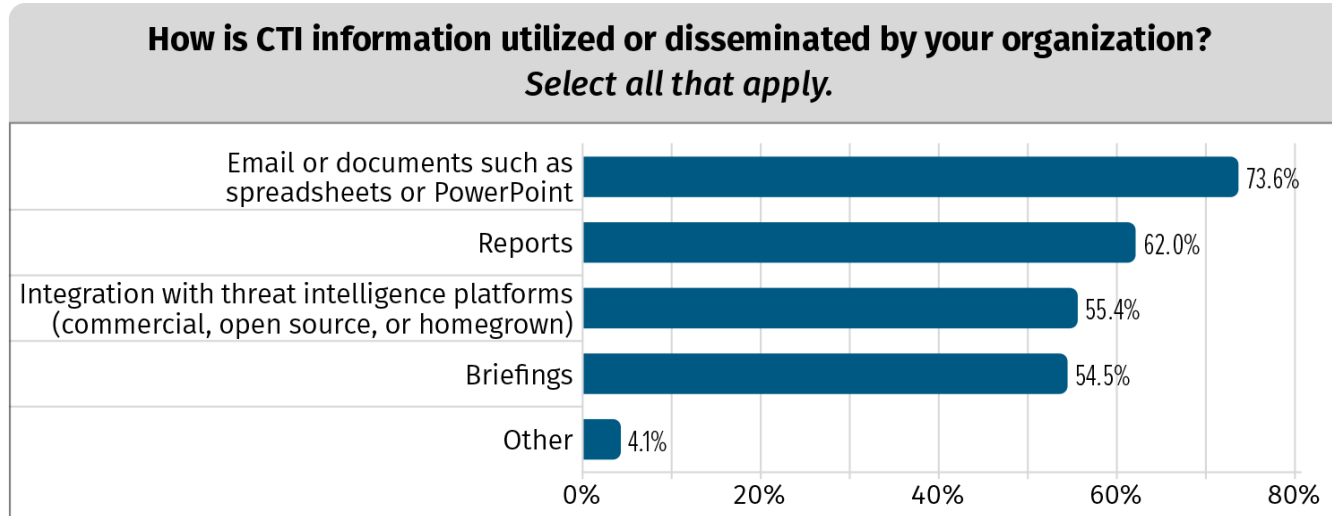
Processing

- Fully-automated: All categories were less than 20%.
- Semi-automated: Enrichment and de-duplication of data were the most leveraged (~40%).
- Manual: Malware analysis is still primarily a manual process.

Analysis



Dissemination



CTI Tools

- Top tools used: Spreadsheets (44%)
- SIEM (40%)
- Network traffic analysis tools (38%)
- Threat intelligence platforms:
 - 56% use a homegrown platform
 - Commercial and open-source platforms (37%)

Moving Forward

- Collaboration and Communication are critical
- Focus on formalizing intuitive-based analysis processes
- Identify tools and systems that will help standardize and optimize CTI processes – including measuring effectiveness and impact.

**EclecticIQ**Intelligence
at the core

Questions or Comments?

Connect with Megan Gooch, *EclecticIQ*

For General Event Discussion:
#discussion

For Sponsor Specific Discussion:
#sponsor-eclecticiq

Observations on Responses from the 2022 SANS CTI Survey

Megan Gooch

Manager, Threat Research | EclecticIQ



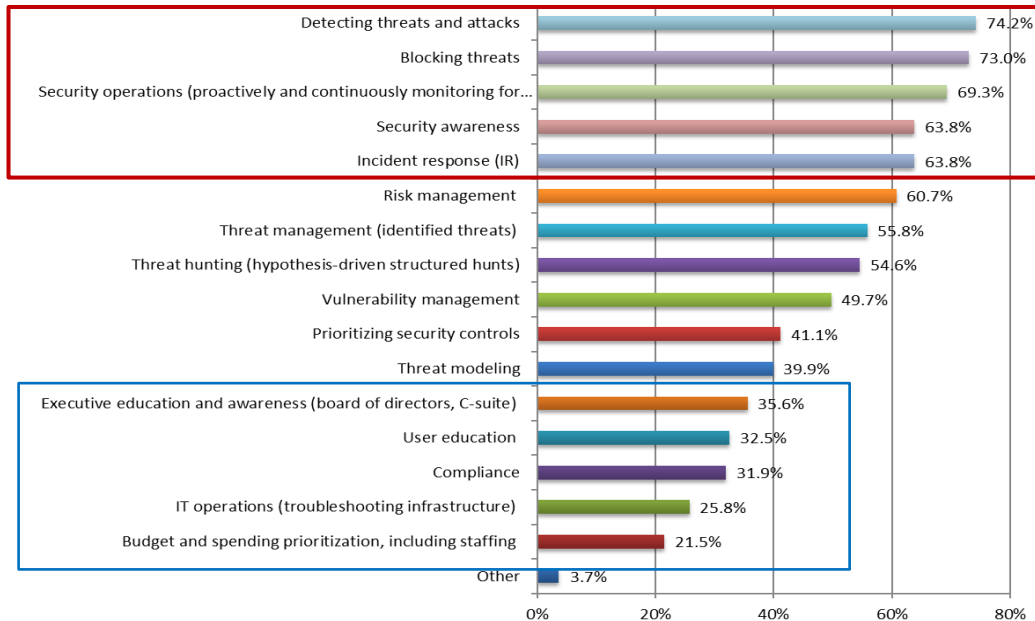
Agenda

23 February 2022

- Survey results through various lenses
 - An Intelligence Analyst
 - Somebody new(er) to the field of CTI
 - A TIP vendor
 - Manager of a vendor company's threat research team

As an Intelligence Analyst

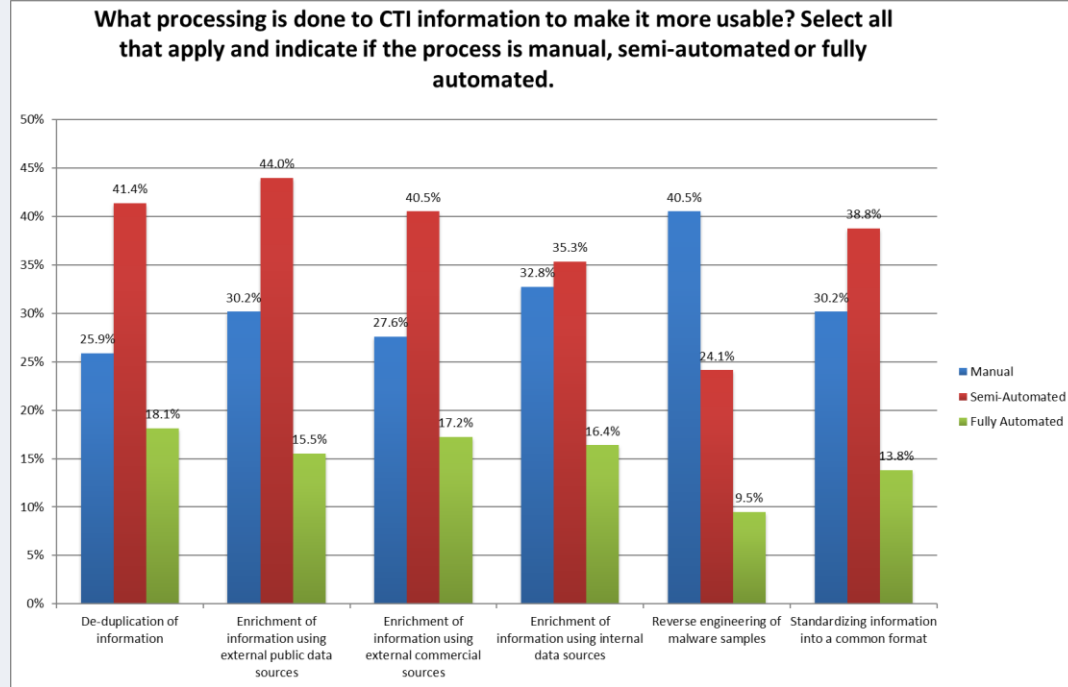
How is CTI data and information being utilized in your organization? Select all that apply.



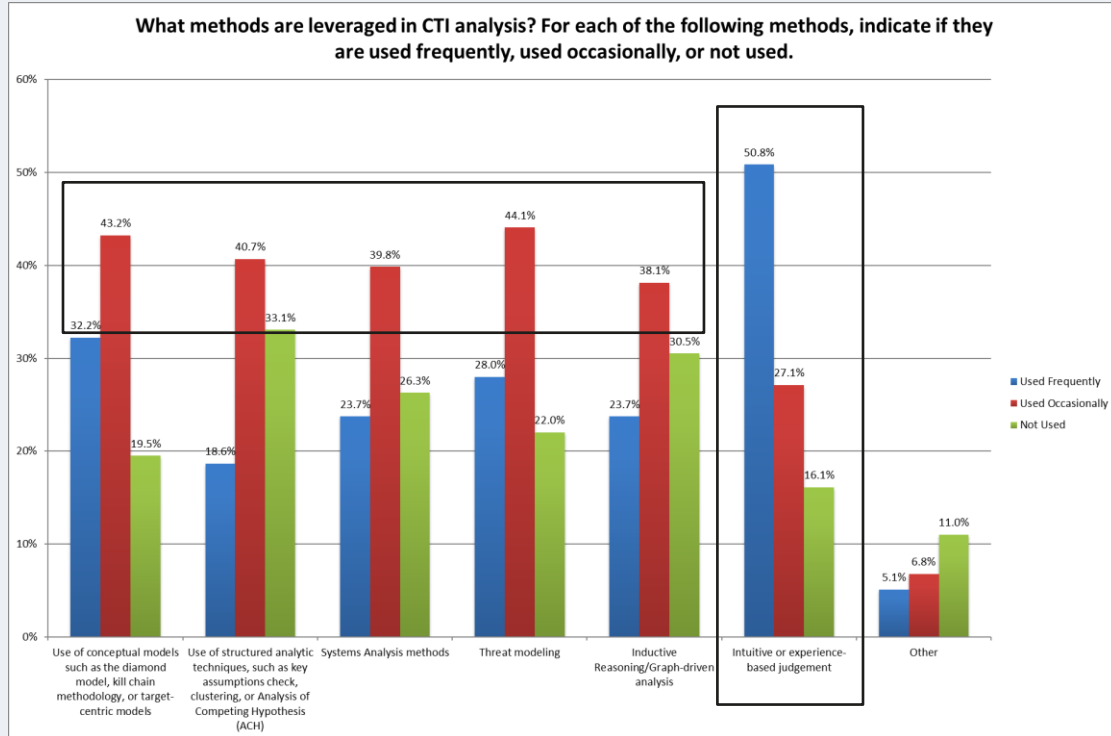
- Every analyst wants to know: what effect did my work have?
- Big differences in the rates of use for tactical versus more strategic tasks

A cyber new-comer

- Most respondents indicate that most processes remain manual or are semi-automated
- The process that is most fully automated is “*de-duplication of information*” [18% of respondents]



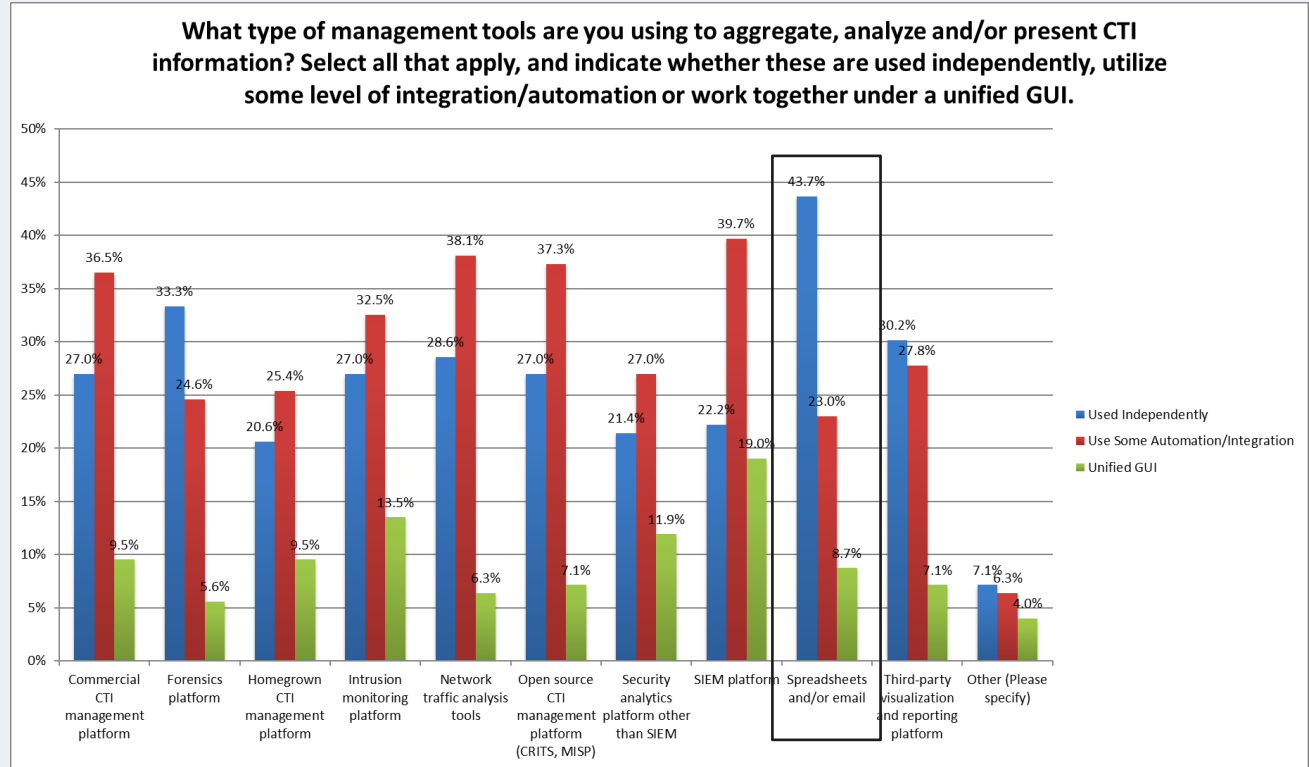
A newcomer, continued....



- Half of respondents indicate “intuitive or experience-based judgement” is used frequently
- Relatively high numbers of occasional use for conceptual models, structured analytic techniques, systems analysis, threat modeling and inductive/graph driven analysis

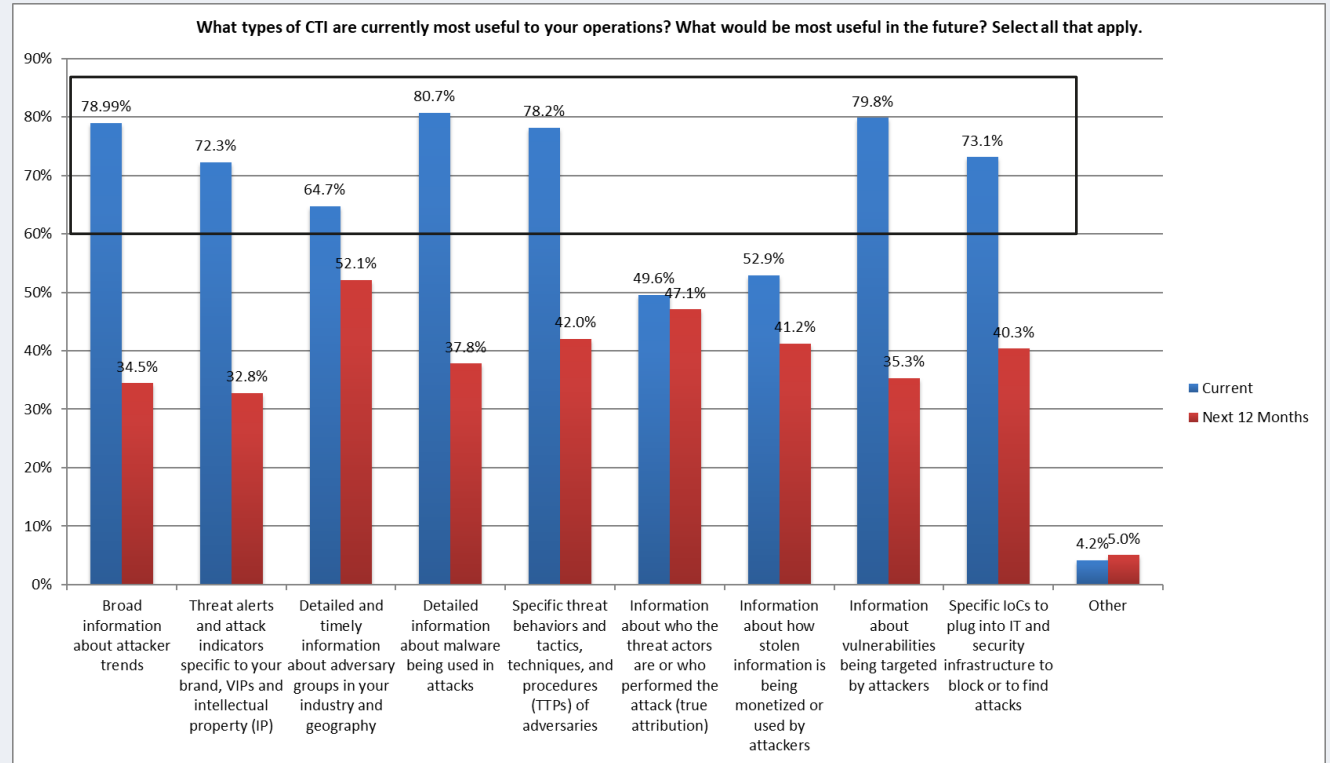
As a vendor

- Responses varied widely – why?
- Single highest response rate for use of a specific tool is for “spreadsheets and/or email”



Manager of a threat research team at a vendor

- Focus on the blue “current” utility scores – very high scores across the board





Infoblox 

Questions or Comments?

Connect with Bob Hansmann, *Infoblox*

For General Event Discussion:
#discussion

For Sponsor Specific Discussion:
#sponsor-infoblox



Demonstrating CTI Value through defense, investigation, and response



Bob Hansmann
Sr. Product Marketing Manager – Security
Infoblox

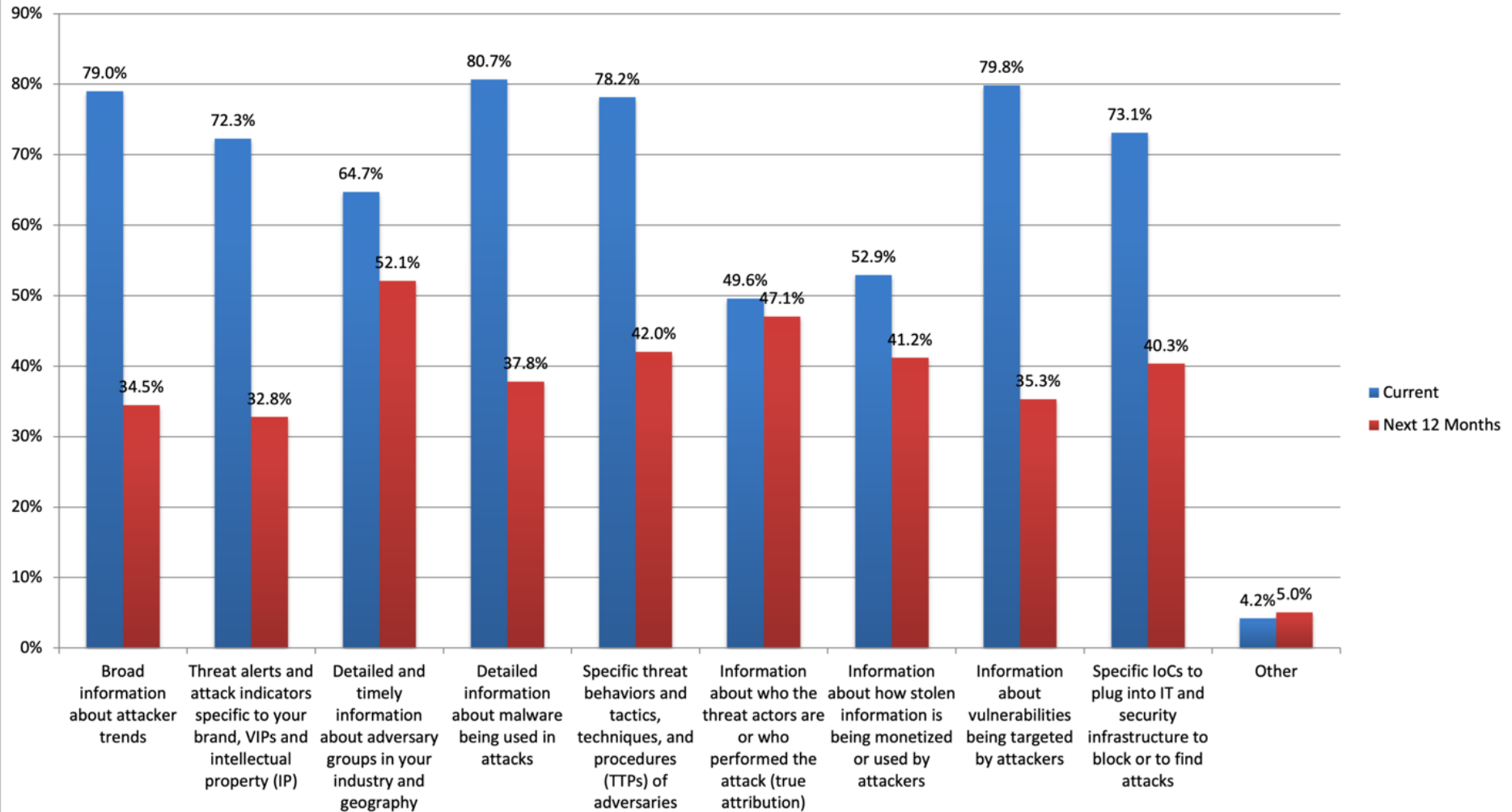


1 in 5 cannot justify their CTI program

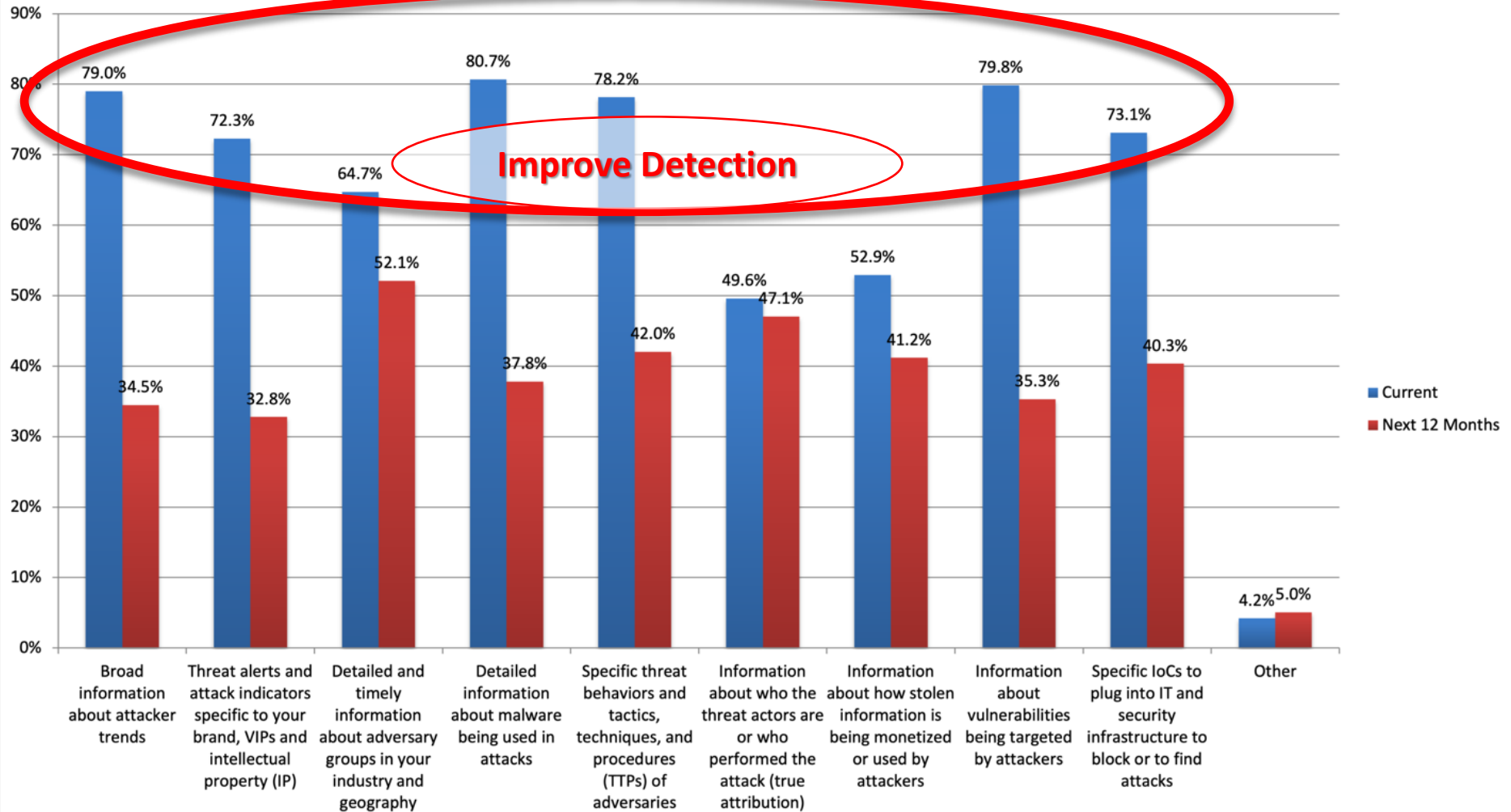
- III. Quite an important percentage of responders, 21%, said they were not able to measure whether their CTI program was indeed useful and valuable to their organizations. This result highlights the need for more and better ways to measure the effectiveness of CTI programs, the tools, and the sources, a call to action for both practitioners and vendors alike, to find better and easier ways to measure CTI success.



What types of CTI are currently most useful to your operations? What would be most useful in the future? Select all that apply.



What types of CTI are currently most useful to your operations? What would be most useful in the future? Select all that apply.



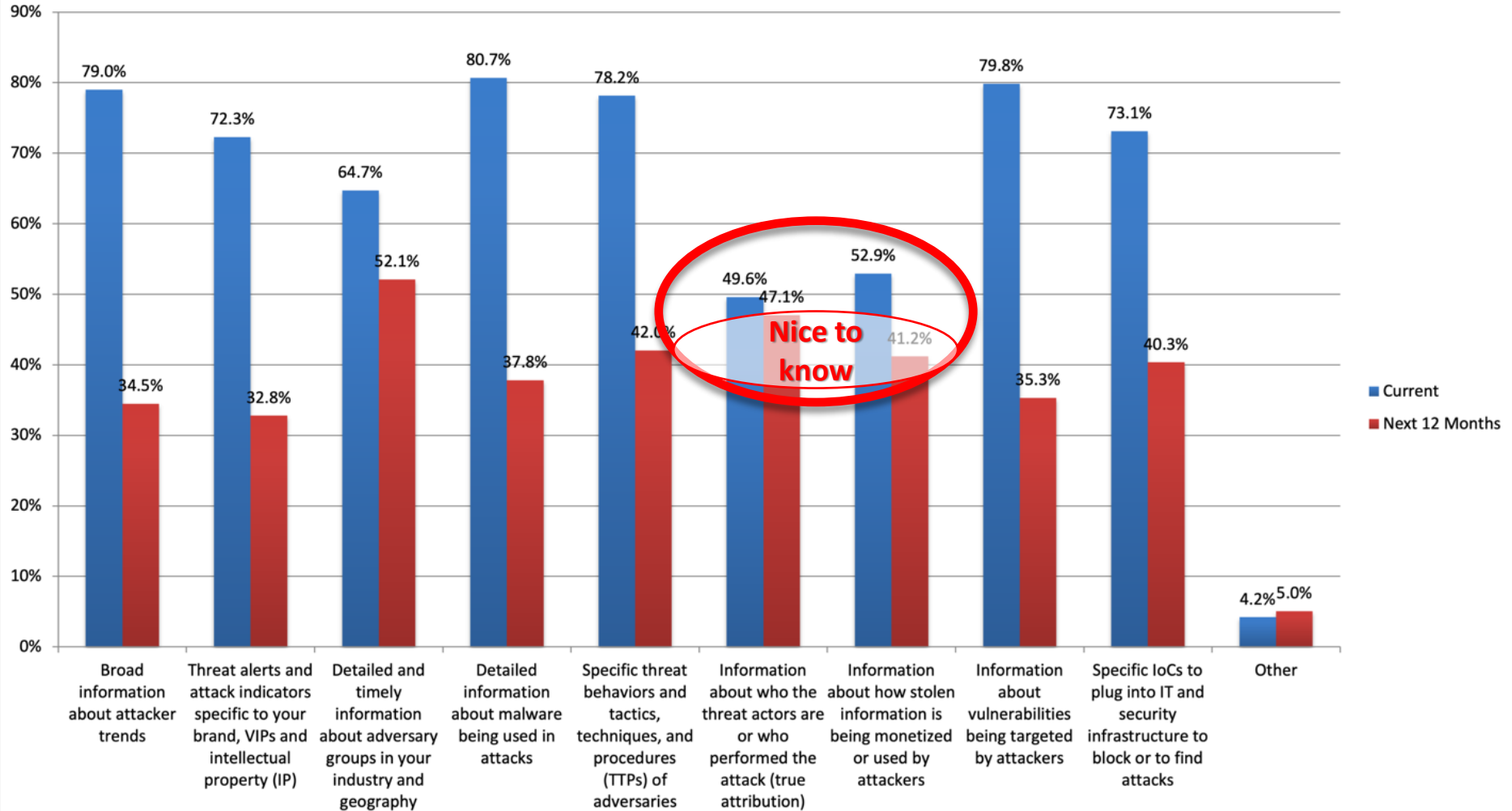
What types of CTI are currently most useful to your operations? What would be most useful in the future? Select all that apply.



Improve Detection


■ Current
■ Next 12 Months

What types of CTI are currently most useful to your operations? What would be most useful in the future? Select all that apply.



For Defense, Time is the Enemy

- Collect the right feeds
 - Industry, regional, etc.
 - Leverage all sources
 - FP Sensitivity
 - Custom lists (Allow/Deny)




A different cup of TI? The added value of commercial threat intelligence

Xander Bouwman, *Delft University of Technology, the Netherlands*; Harm Griffioen, *Hasso Plattner Institute, University of Potsdam, Germany*; Jelle Egbers, *Delft University of Technology, the Netherlands*; Christian Doerr, *Hasso Plattner Institute, University of Potsdam, Germany*; Bram Klievink, *Leiden University, the Netherlands*; Michel van Eeten, *Delft University of Technology, the Netherlands*

<https://www.usenix.org/conference/usenixsecurity20/presentation/bouwman>

This paper is included in the Proceedings of the
29th USENIX Security Symposium.
August 12–14, 2020
978-1-939133-17-5



**Reading the Tea leaves:
A Comparative Analysis of Threat Intelligence**

Vector Guo Li, *University of California, San Diego*; Matthew Dunn, *Northeastern University*; Paul B. ...; Damon McCoy, *New York University*; Geoffrey M. Voelker and ...; Kirill Levchenko, *University of Illinois Urbana-Champaign*

<https://www.usenix.org/conference/usenixsecurity19/presentation/li>

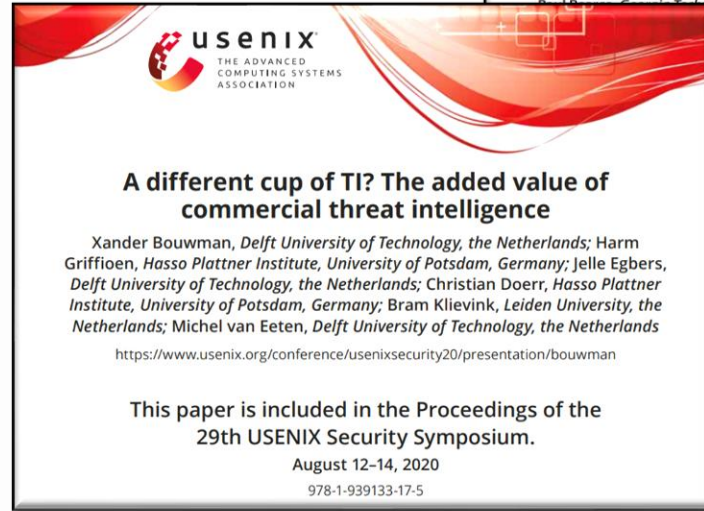
This paper is included in the Proceedings of the
28th USENIX Security Symposium.
August 14–16, 2019 • Santa Clara, CA, USA
978-1-939133-06-9

Open access to the Proceedings of the
28th USENIX Security Symposium
is sponsored by USENIX.



For Defense, Time is the Enemy

- Collect the right feeds
 - Industry, regional, etc.
 - Leverage all sources
 - FP Sensitivity
 - Custom lists (Allow/Deny)



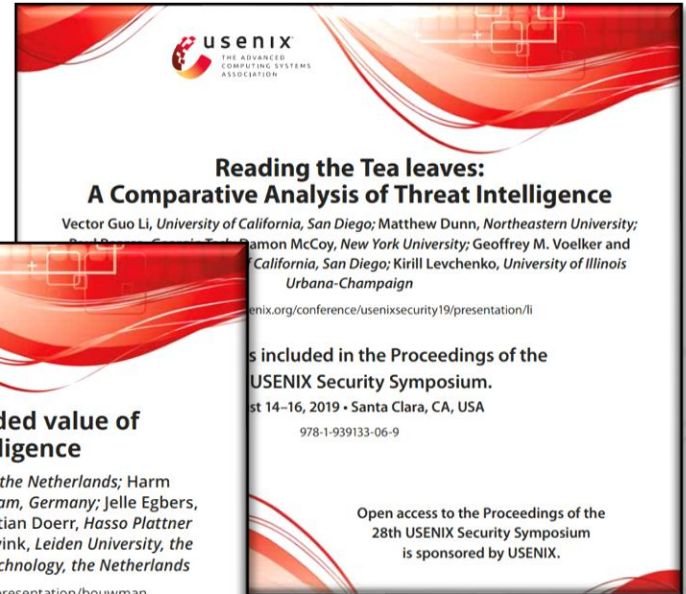
usenix
THE ADVANCED
COMPUTING SYSTEMS
ASSOCIATION

A different cup of TI? The added value of commercial threat intelligence

Xander Bouwman, *Delft University of Technology, the Netherlands*; Harm Griffioen, *Hasso Plattner Institute, University of Potsdam, Germany*; Jelle Egbers, *Delft University of Technology, the Netherlands*; Christian Doerr, *Hasso Plattner Institute, University of Potsdam, Germany*; Bram Klievink, *Leiden University, the Netherlands*; Michel van Eeten, *Delft University of Technology, the Netherlands*

<https://www.usenix.org/conference/usenixsecurity20/presentation/bouwman>

This paper is included in the Proceedings of the
29th USENIX Security Symposium.
August 12–14, 2020
978-1-939133-17-5



usenix
THE ADVANCED
COMPUTING SYSTEMS
ASSOCIATION

Reading the Tea leaves: A Comparative Analysis of Threat Intelligence

Vector Guo Li, *University of California, San Diego*; Matthew Dunn, *Northeastern University*; Paul Bracken, *George Mason University*; Damon McCoy, *New York University*; Geoffrey M. Voelker and
University of California, San Diego; Kirill Levchenko, *University of Illinois Urbana-Champaign*

<https://www.usenix.org/conference/usenixsecurity19/presentation/li>

This paper is included in the Proceedings of the
28th USENIX Security Symposium.
August 14–16, 2019 • Santa Clara, CA, USA
978-1-939133-06-9

Open access to the Proceedings of the
28th USENIX Security Symposium
is sponsored by USENIX.

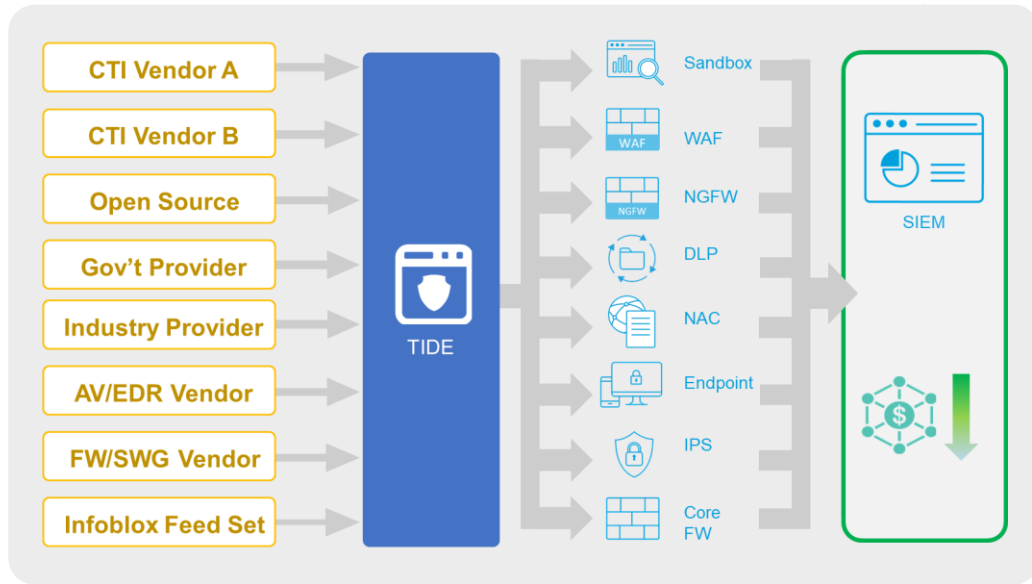
**Maximum observed overlap
between feeds was only 11%!**



For Defense, Time is the Enemy

- Collect the right feeds
 - Industry, regional, etc.
 - Leverage all sources
 - FP Sensitivity
 - Custom lists (Allow/Deny)
- Automate distribution

Get IoCs out fast!



For IR, Time is the Enemy

- Make TI Accessible
- Framework alignment (i.e. ATT&CK)

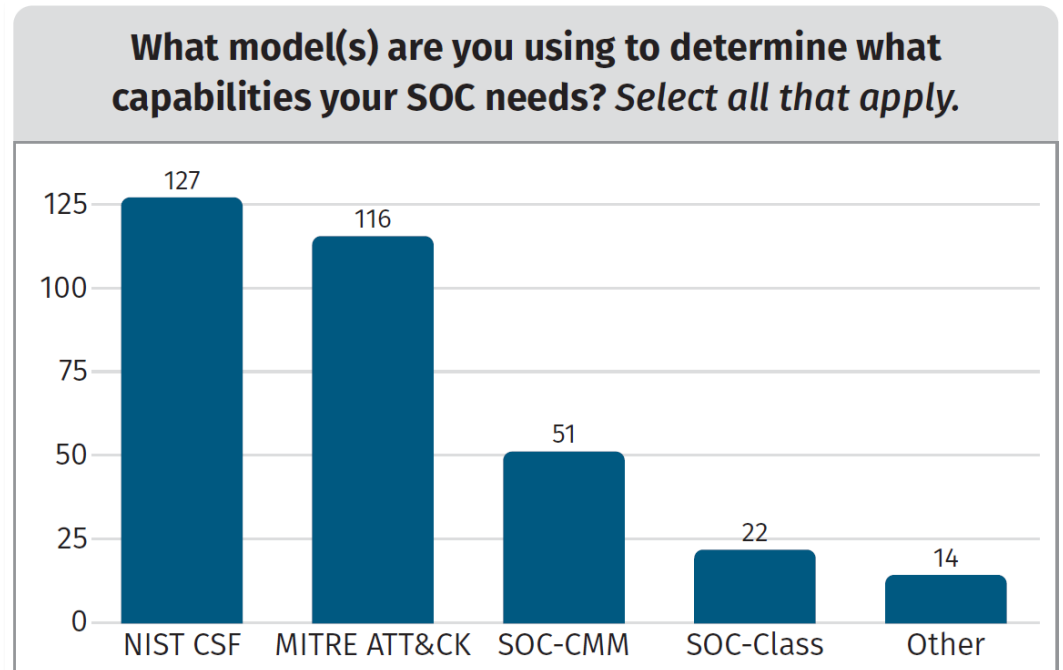


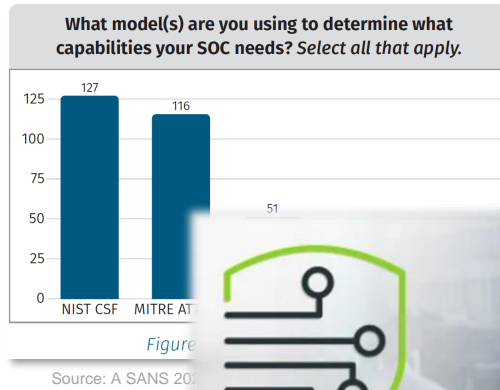
Figure 10. Capability Model in Use (Q15 n=241)

Source: A SANS 2021 Survey: Security Operations Center (SOC)



For IR, Time is the Enemy

- Make TI Accessible
- Framework alignment (i.e. ATT&CK)
- Auto Correlate TI with
 - Events/Incidents
 - Device data (DHCP, Discovery, IPAM)

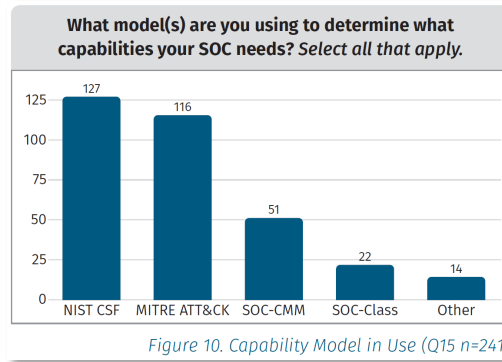


Reduce investigation time by up to 2/3rds!



For IR, Time is the Enemy

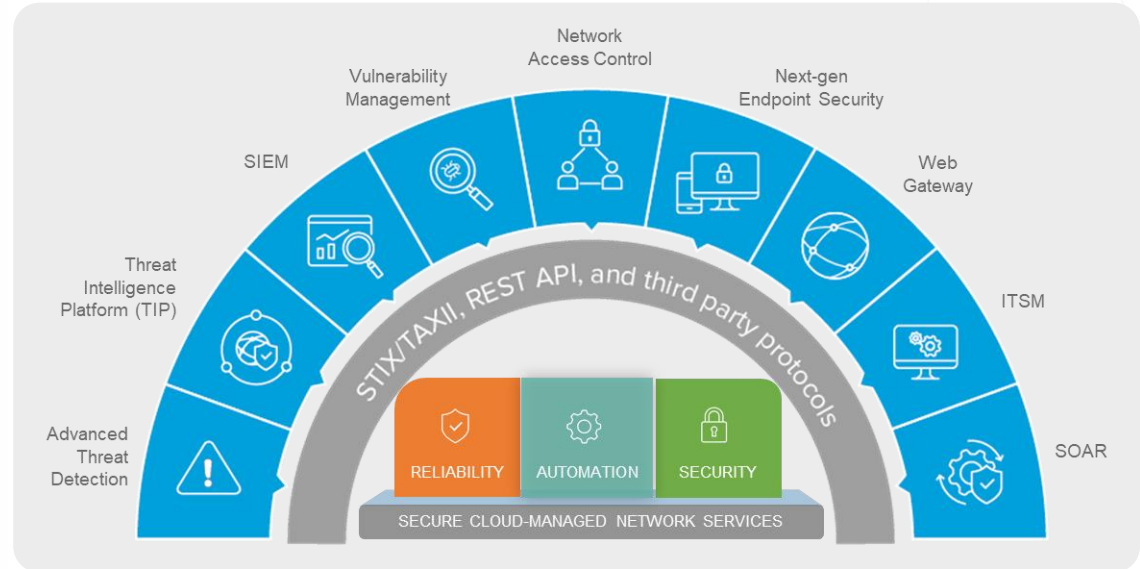
- Make TI Accessible
- Framework alignment (i.e. ATT&CK)
- Auto Correlate TI with
 - Events/Incidents
 - Device data (DHCP, Discovery, IPAM)
- Early Automation
 - Trigger Vuln. Scans
 - VLAN Isolation



Source: A SANS 2021 Survey: Security Operations Center (SOC)



Reduce investigation time by up to 2/3rds!



Leverage Automation

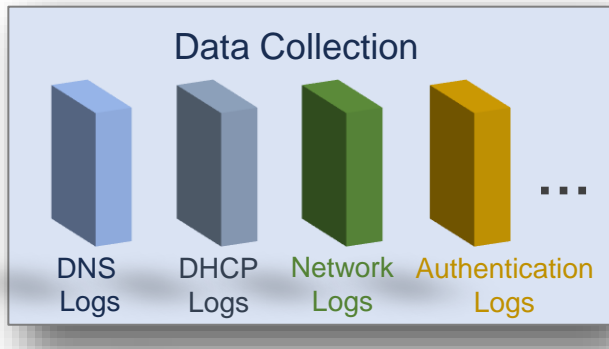


Typical Threat Investigation / Incident Response

1. Threat teams receive thousands of alerts every day
 - Each alert is typically identified by an IP address



Typical Threat Investigation / Incident Response



1. Threat teams receive thousands of alerts every day

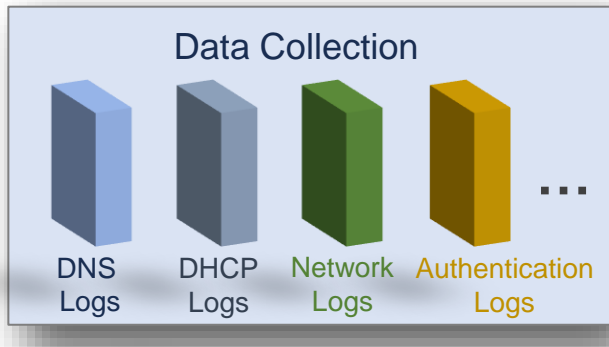
- Each alert is typically identified by an IP address

2. Manually collect logs from multiple systems

- Automation is a challenge (access & storage requirements)



Typical Threat Investigation / Incident Response



1. Threat teams receive thousands of alerts every day

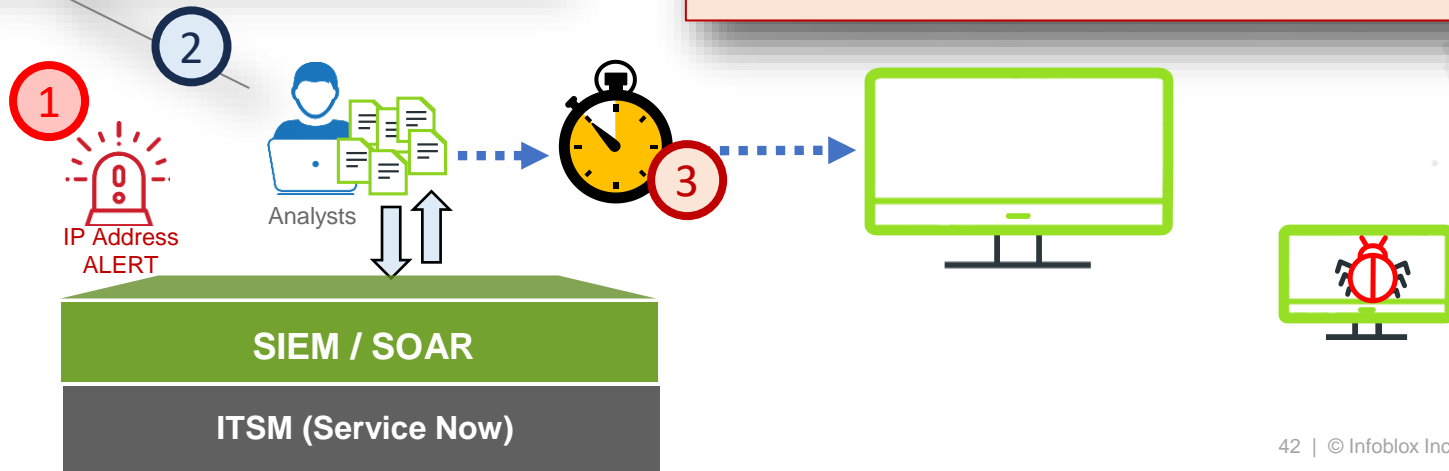
- Each alert is typically identified by an IP address

2. Manually collect logs from multiple systems

- Automation is a challenge (access & storage requirements)

3. Correlation takes additional time

- Current, reliable data needed to confidently identify systems

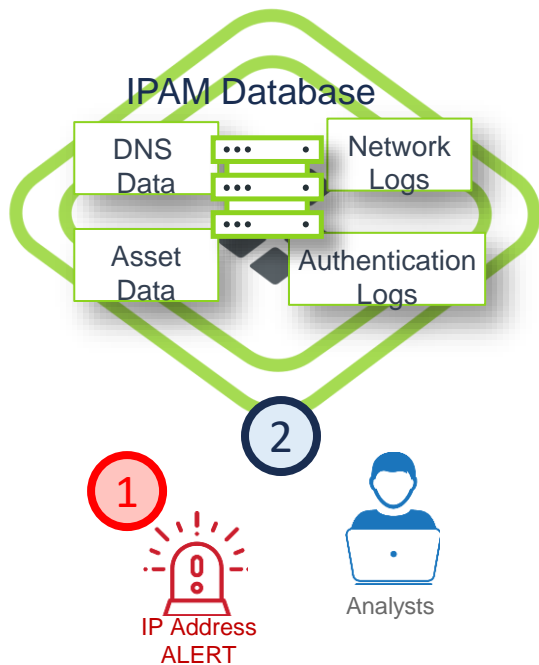


Incident Response with Infoblox DDI + NetMRI

1. Threat teams receive thousands of alerts every day
 - Each alert is typically identified by an IP address



Incident Response with Infoblox DDI + NetMRI



1. Threat teams receive thousands of alerts every day

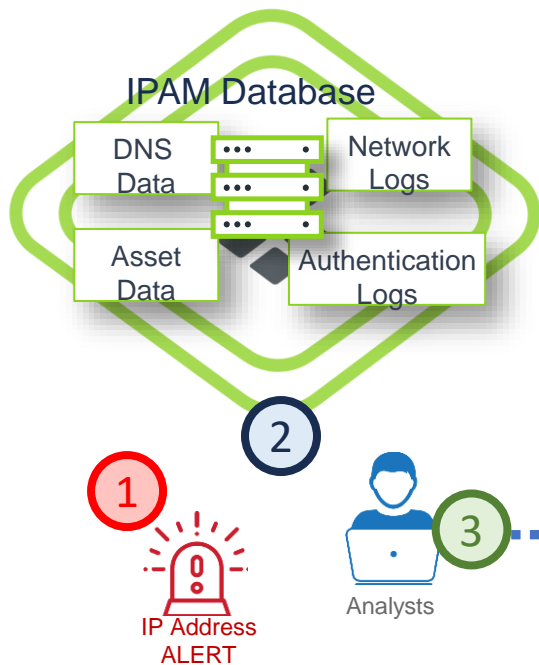
- Each alert is typically identified by an IP address

2. Lookup IP Address Management (IPAM) database (DDI)

- Automatically Translates IP address to: **device**, **user** and **network location**



Incident Response with Infoblox DDI + NetMRI



1. Threat teams receive thousands of alerts every day

- Each alert is typically identified by an IP address

2. Lookup IP Address Management (IPAM) database (DDI)

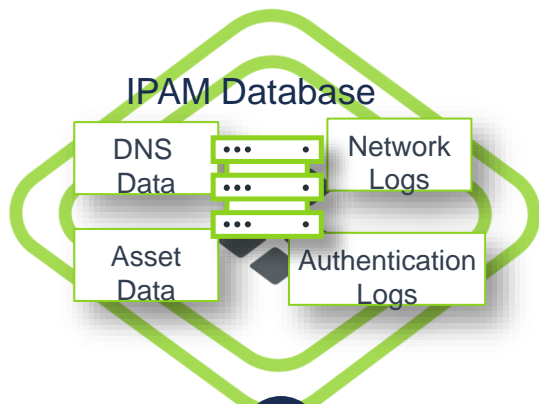
- Automatically Translates IP address to: **device**, **user** and **network location**

3. Immediately identify compromised device(s)

- Remediate significantly faster with accuracy



Incident Response with Infoblox DDI + NetMRI



1. Threat teams receive thousands of alerts every day

- Each alert is typically identified by an IP address

2. Lookup IP Address Management (IPAM) database (DDI)

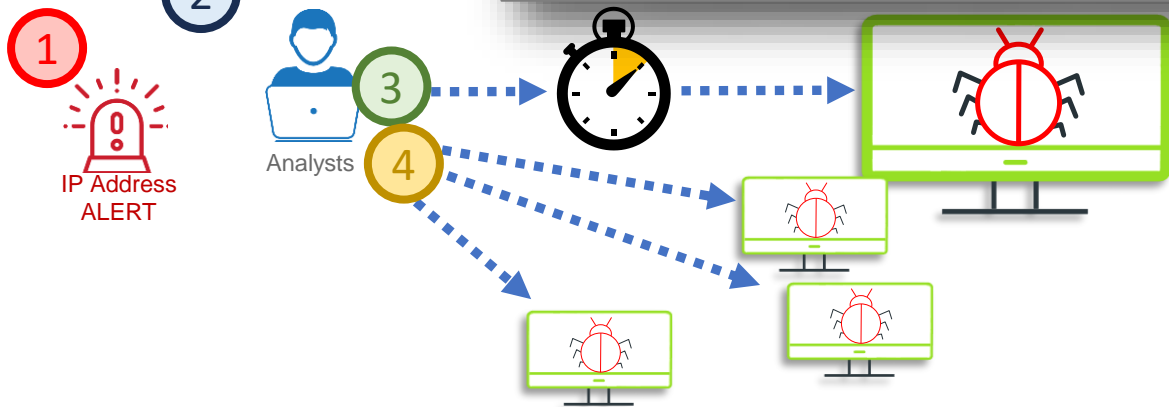
- Automatically Translates IP address to: **device**, **user** and **network location**

3. Immediately identify compromised device(s)

- Remediate significantly faster with accuracy

4. Identify scope of threat exposure

- Quickly identify other systems communicating with same threat locations





Questions or Comments?

Connect with David Monnier, *Team Cymru*

For General Event Discussion:
#discussion

For Sponsor Specific Discussion:
#sponsor-team-cymru





**David Monnier, Team Cymru Fellow
and Head of Infrastructure and
Services**

Our clients spoke; the three biggest issues they are dealing with

Email Protection Gaps



**Determining
between valid and
phishing emails
continues to be an
issue**

Alert Triage



**Context and alert
validity remain
challenging**

Ransomware



**Modern ransomware
is evolving**

How Pure Signal Recon gives you an advantage



Threat Intelligence vs. Threat Hunting vs. Threat Reconnaissance

Threat Intelligence

Threat Hunting

Threat Reconnaissance

(dns|resolve)
.adobelicence.com

45.105.134.228



185.174.100.56



(dns|resolve)
.msnconnection.com

213.23.113.190



217.79.185.65

(www).zygma.ir

(www).seyyedalihosseini.com

(ns1|ns2).hanistech.com

TCP 80/443

UDP:23

77.42.48.104

21 22 80



TCP/22

51.15.253.189

159.65.8.14

107.170.72.240

138.201.147.13

51.15.248.235

175.227.87.190

207.154.195.24

138.201.180.14

UDP/21

TCP/22

77.42.33.247

21 22 80



TCP/2

213.5.70.19

167.99.248.21

TCP 25

195.201.115.20

159.65.125.225

159.89.27.225

46.143.112.22

80



TCP 69

TCP 66

5.221.91.148

80



UDP 25

159.89.27.225




2.191.56.254


80



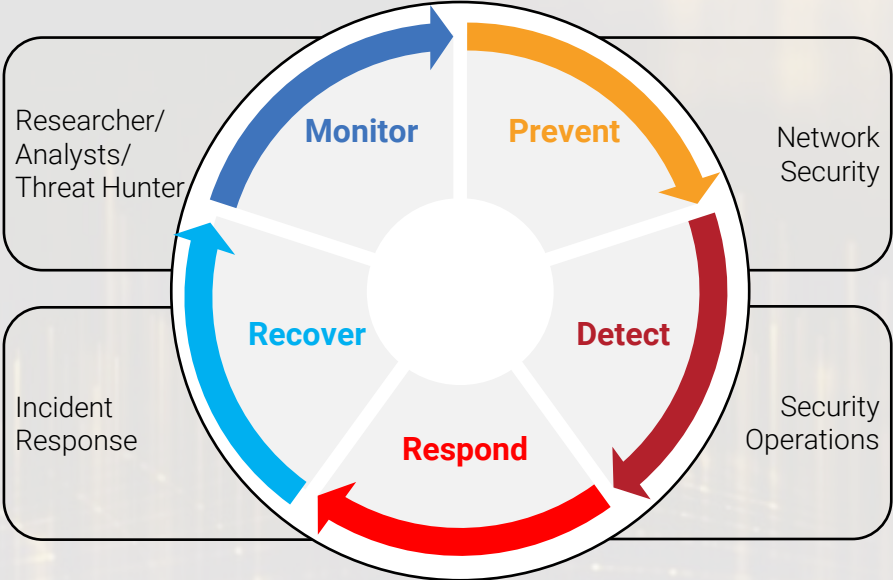
TCP 22

UDP 23

 MALICIOUS C2 INFRASTRUCTURE

 VICTIMS

Common Threat Intelligence Challenges



Visibility ends at the firewall
Threat intel isn't comprehensive,
and it's dated

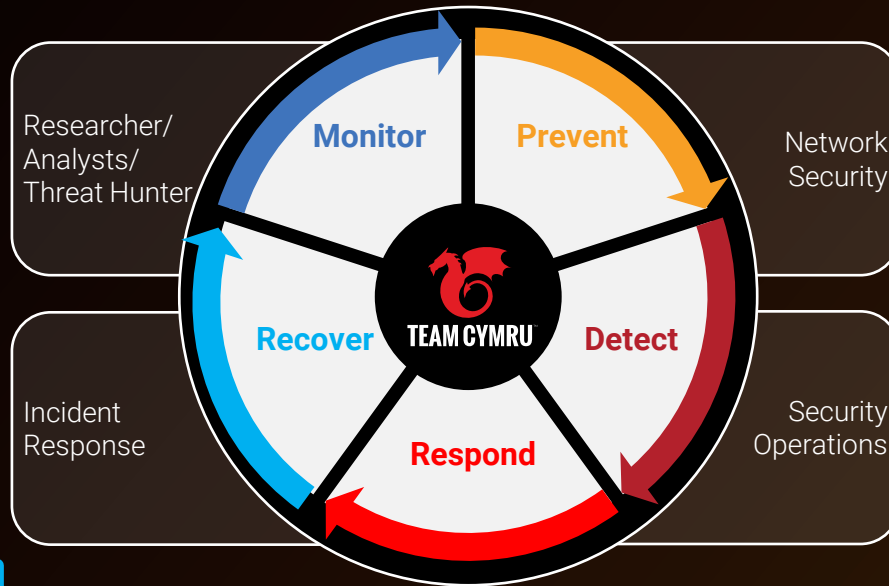
Email protection tools don't stop
all phishing emails

Remediation success is a
challenge

IR team lacks visibility

Chasing yesterday's threats
today
Threats evolve faster than
security vendors can track

Threat Hunting efforts that yield lasting defense outcomes



Trace, map and monitor adversary infrastructure

Monitor third parties for signals of compromise

Proactively block adversary infrastructure

Improve block list accuracy

Post recovery clean up validation

Prevent repeat attacks from same actor

Use observations of victims to take proactive defensive measures

Accelerate compromise assessment

Reduce SOC 'noise' and false positive/negative resource drain

Observe malicious C2 connections missed by security tools

Tangible value to our customers

Fortune 50 Case Study

**\$9.03m
Savings**



Data Breach
Risk Reduction



Managing
Compromised
Third-Party Threats



Averted Attack From
Compromised Acquisition



Consolidation of
Threat Intelligence Services



Reducing Operation Drain
From Phishing Attacks

**Forrester Consulting Quantified
Gains**

Relied upon by elite security teams worldwide

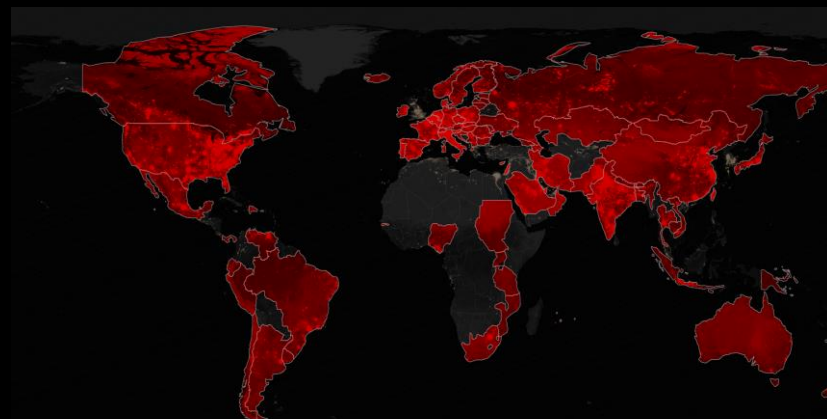


THANK YOU



Who we are;

- **Founded in 2005**
- **Mission:**
- **To save and improve human lives.**
- **Unmatched eco-system of data sharing partnerships worldwide.**
- **Work with 130+ CSIRT teams in 86+ countries**
- **Relied on by many security vendors, Fortune 100 companies, and public sector entities.**

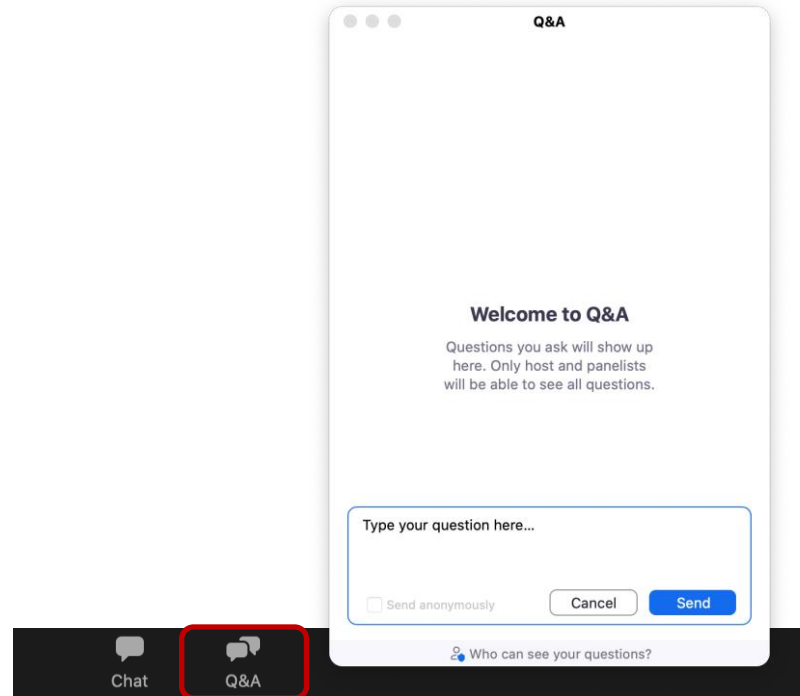


CSIRT Support Coverage Map

Q&A

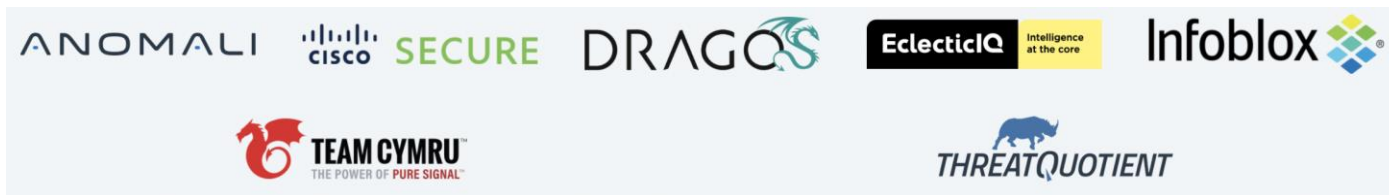
Please use **Zoom's** Q&A window to submit questions to our presenters.

Type your question, tell us if it's for a specific presenter, and then click Send.



Acknowledgments

Thanks to our sponsors:



To our special guests: Megan Gooch, Bob Hansmann, David Monnier

And to our attendees, thank you for joining us today!