.conf18

splunk>

Assessing Threat Intelligence from Sharing Communities

A review and analysis approach

Ken Towne | Global Resilience Federation
Glenn Wong | Recorded Future

Forward-Looking Statements

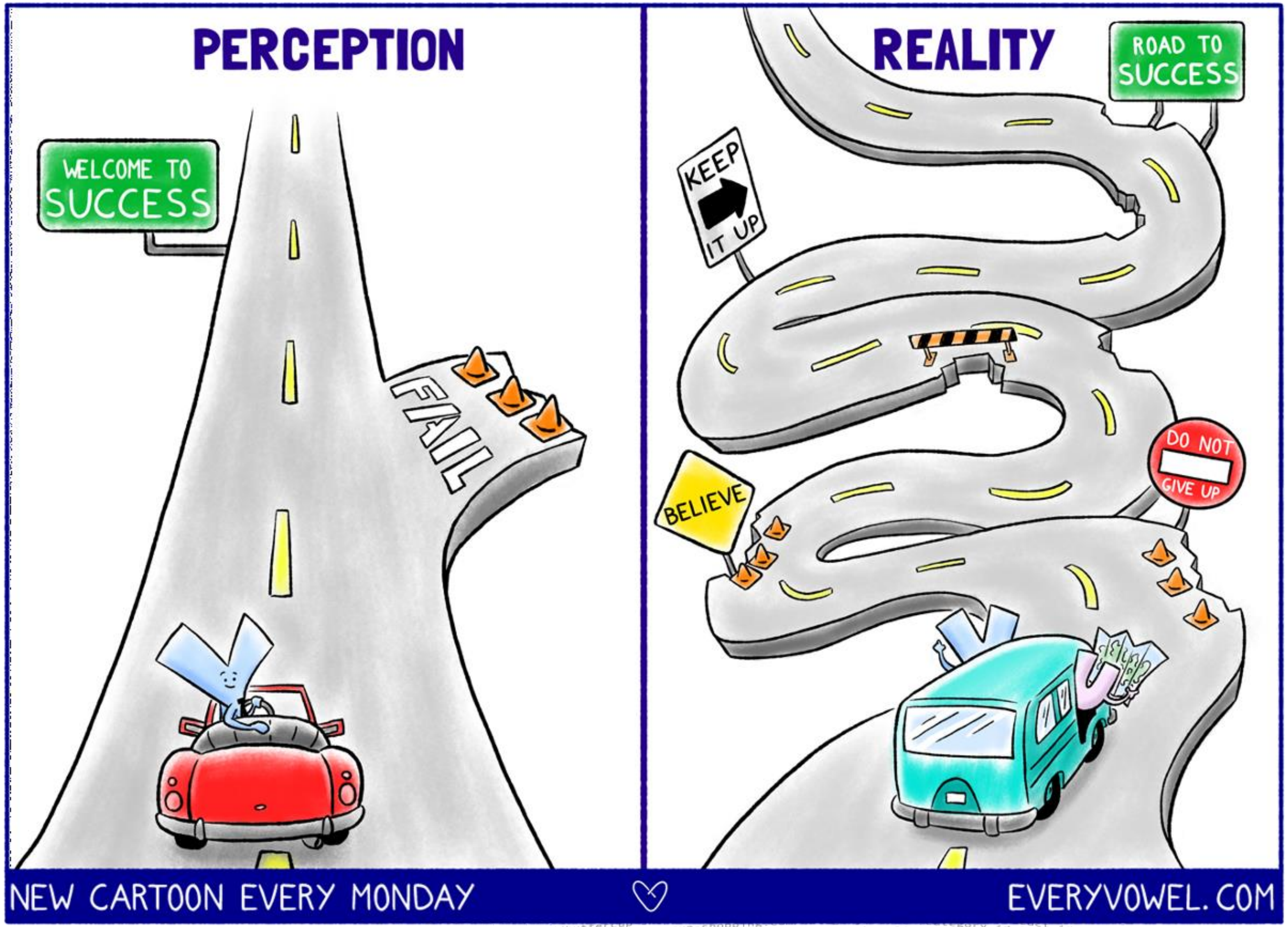
During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Agenda

- Introduction – Sharing Communities
- Need for Assessment
- Analysis Methodology
- Results
- Impact and Next Steps

SHARING THREAT INTELLIGENCE



OVERVIEW OF ISACs, ISAOs

ISAC

- Information Sharing and Analysis Centers (ISACs), as defined by EO 12472 and the national critical infrastructure protection goals of Presidential Decision Directive 63 (PDD-63), were already essential drivers of effective cyber security collaboration for specific industrial sectors such as banking and financial services, energy, telecommunications and defense, as examples. ISACs are trusted entities established by Critical Infrastructure Key Resource (CI/KR) owners and operators to provide comprehensive sector analysis, which is shared within the sector, with other sectors, and with government.

ISAO

- An Information Sharing and Analysis Organization (ISAO) is a group created to gather, analyze, and disseminate cyber threat information. Unlike ISACs, ISAOs are not directly tied to critical infrastructure sectors, as outlined in Presidential Policy Directive 21. Instead, ISAOs offer a more flexible approach to self-organized information sharing activities amongst communities of interest such as small businesses across sectors: legal, accounting, and consulting firms that support cross-sector clients, etc.

OVERVIEW OF GRF

GRF

- The Global Resilience Federation (GRF) is a private sector non-profit organization that brings together Intelligence organizations to collect, analyze and share cyber and physical threat intelligence for mutual defense. GRF works with members to analyze and mitigate risks in ways that complement companies' own efforts; from tracking systems vulnerabilities to providing in-depth reporting. GRF works to enrich security products and strengthen the overall awareness and actionability of global threat intelligence. GRF provides reports to CSOs and CISOs while exchanging cross-sector intelligence within a multi-industry defensive network of more than 7,000 organizations. Intelligence is drawn from other ISACs and ISAOs, government partners, and private vendors curated independently, collaborated, and trust intelligence source providers tailored toward its supported industry focus'.

Challenges in Assessing Shared Threat Data

Multiple standards

Despite industry attempts to s standardize threat sharing, multiple formats still exist

Arbitrary confidence

Proprietary and non-proprietary methods are used to assign confidence and risk scores

Source reputation

No consistent way to assess validity and importance of different sources

Industry impact

Threat Intelligence can have varying applicability across industries

One size does not fit all

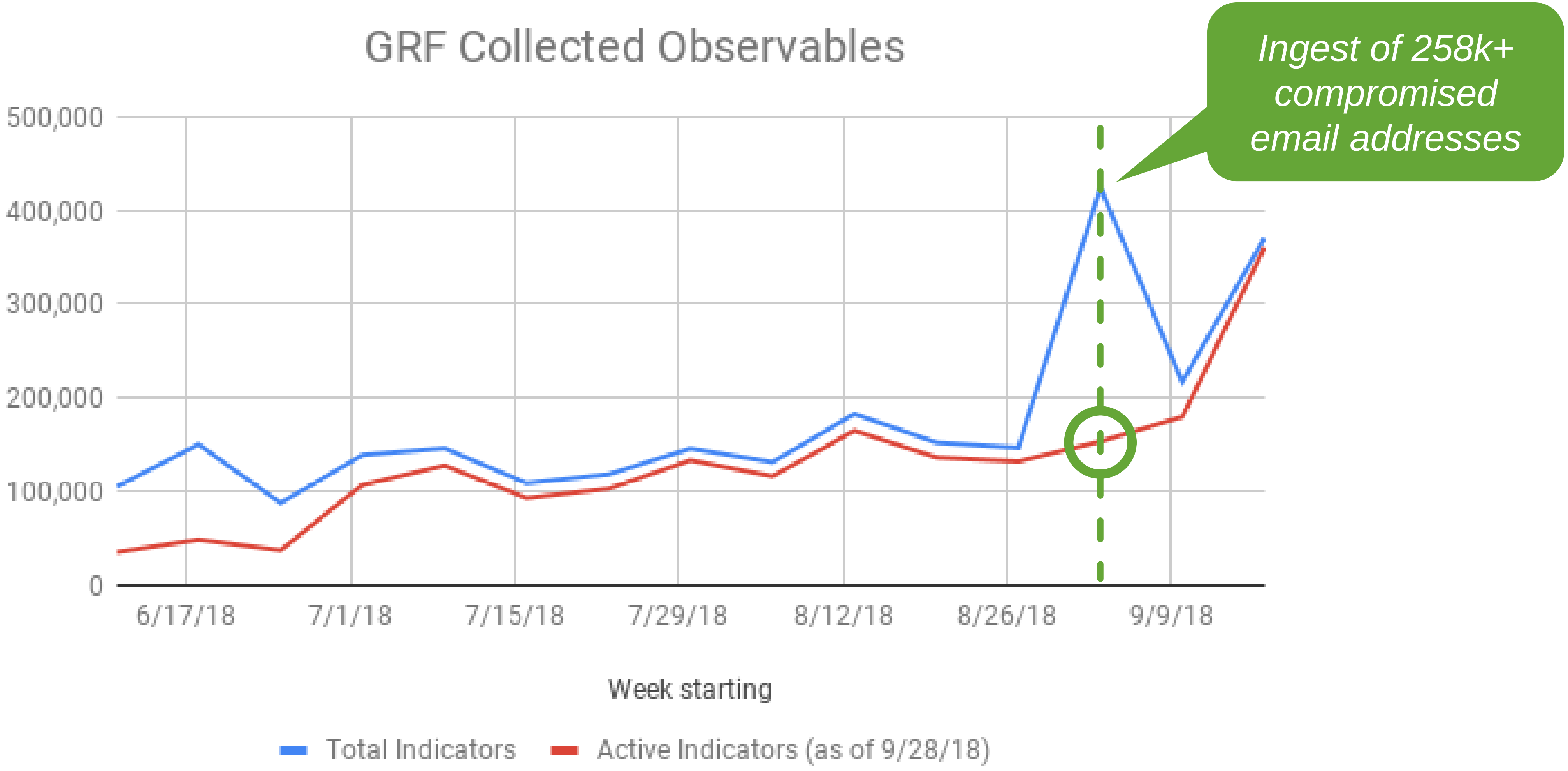
Members/Customers have diverse risks, infrastructure, and tools for leveraging Threat Intelligence

METHODOLOGY

- Pull representative sample of data from GRF repository
  - IP addresses, Hashes, domains
  - Multiple sources, including sharing communities, open sources, and commercial third parties
  - Enrich with additional metrics and information [from Recorded Future]

- Review
  - Descriptive statistics on collected data
  - Determine similarities and differences among different sources and scoring methods

GRF typically processes 100k-200k observables / week

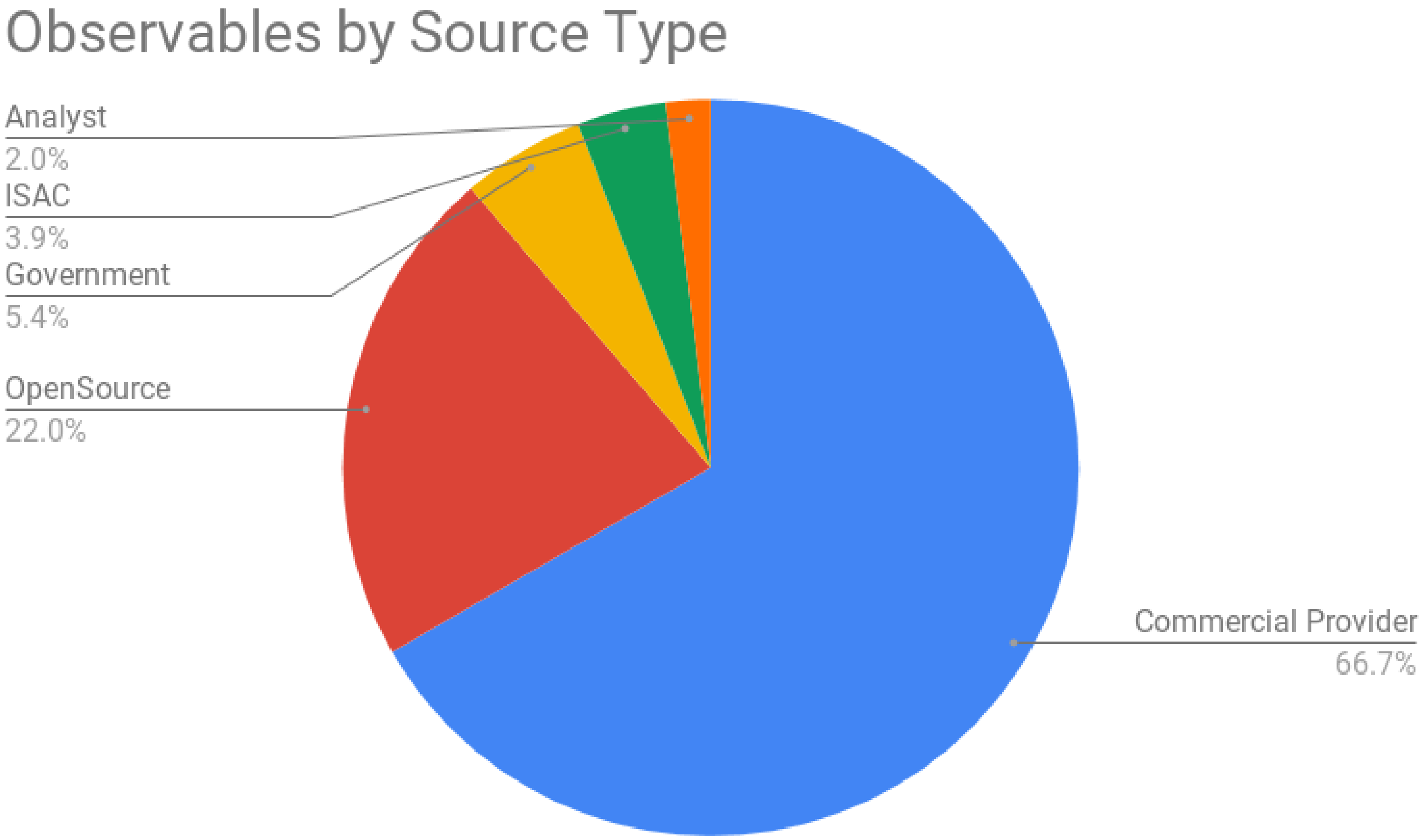


Ingest of 258k+ compromised email addresses

GRF’S collection comes from a wide range of sources

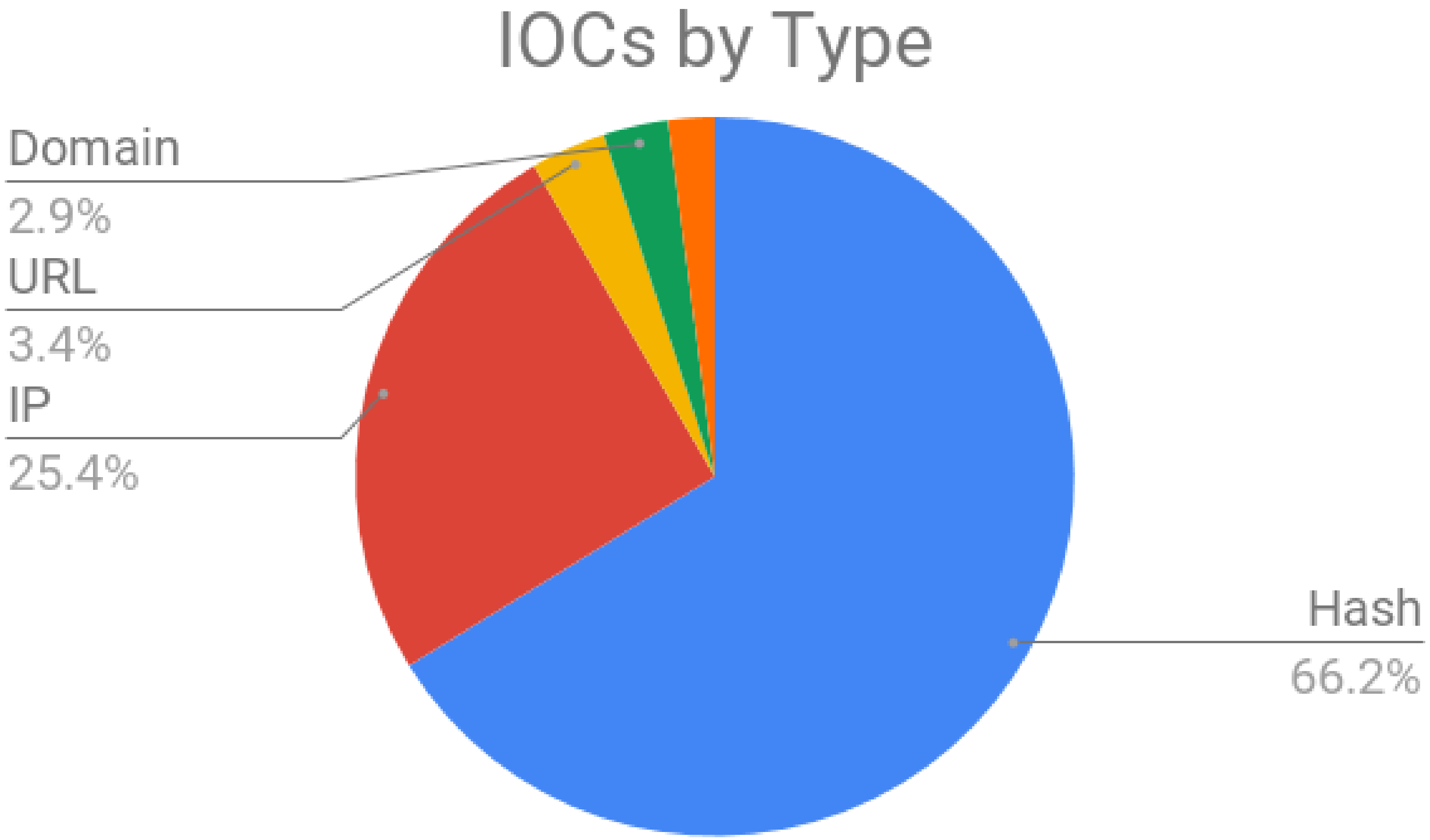
Source Type	# of feeds	# of IOCs 9/3/18-9/10/18	% of Total IOCs
Analyst	1	2,956	2%
Commercial	8	99,895	67%
Government	3	8,133	5%
ISAC	4	5,835	4%
Open Source	45	33,029	22%
SANS	3	14	0%
TOTAL	**64**	**149,862**	**100%**

2/3 of IOCs from Commercial Providers; 1/4 from OSINT



SourceType	*count*
Commercial Provider	99,895
OpenSource	33,029
Government	8,133
ISAC	5,835
Analyst	2,956
SANS	14
TOTAL	**149,862**

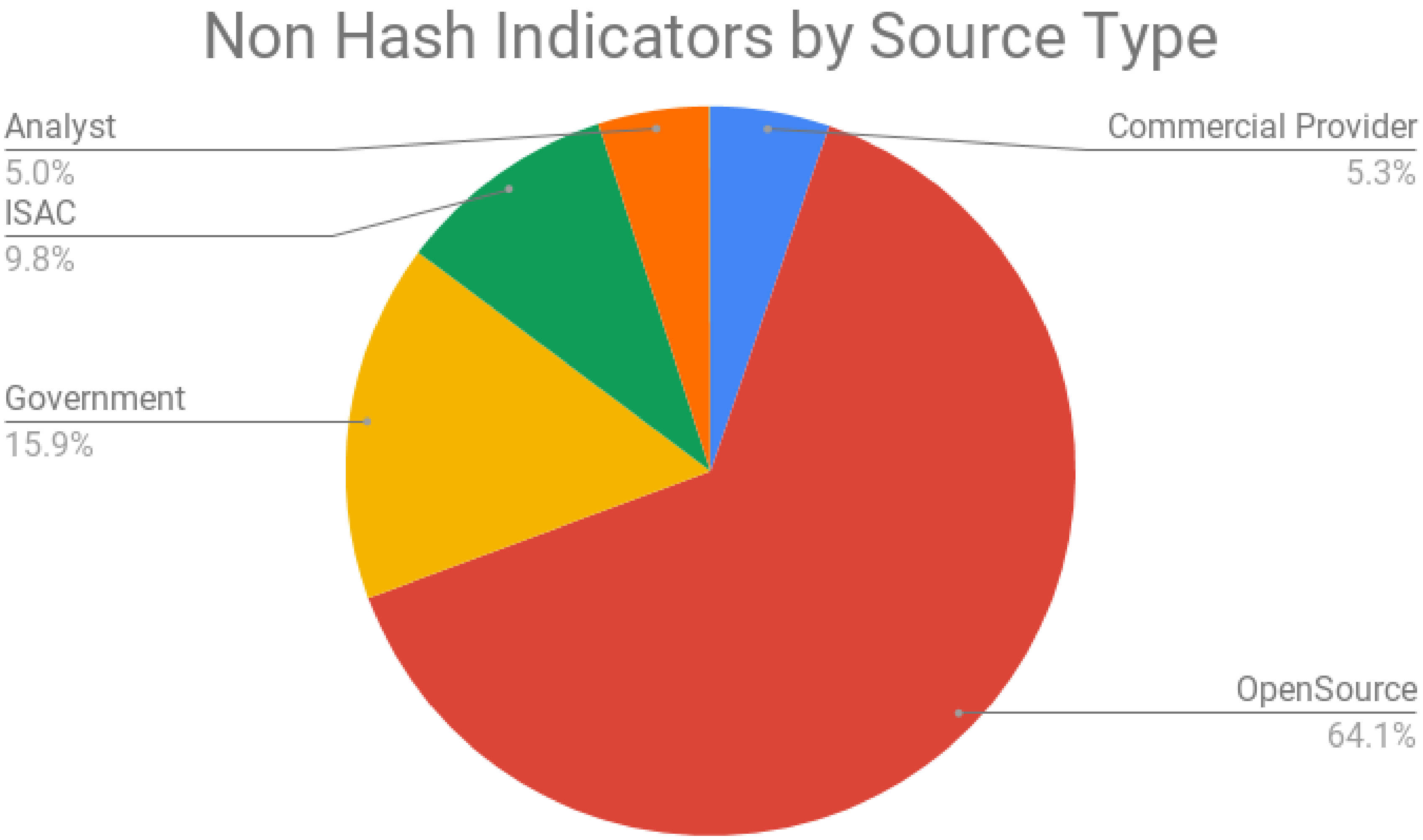
2/3 of Observables are Hashes; 1/4 are IPs



IOCtype	*count*
Hash	99,182
IP	38,109
URL	5,078
Domain	4,371
Other	3,122
TOTAL	**149,862**

* *Active Observables as of 9/28/18 collected from Sept 3-10, 2018*

~2/3 of non-hash threat intel is from open source



SourceType	*count*
OpenSource	32,470
Government	8,055
ISAC	4,961
Commercial Provider	2,671
Analyst	2,509
SANS	14
TOTAL	**50,680**

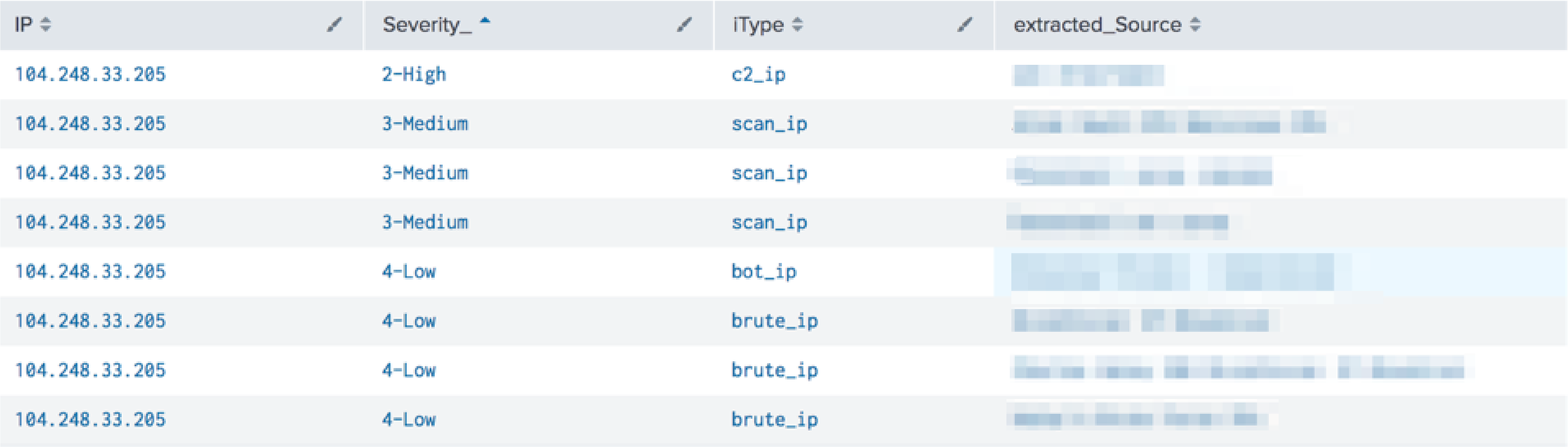
Coverage Overlap varies by IOC type

IOC Type	# of unique entries	# records	% unique IOCs
URL	1,588	5,078	31%
Domain	2,078	4,371	47%
IP	32,535	38,109	85%
Hash	97,420	99,182	98%

Some considerations:

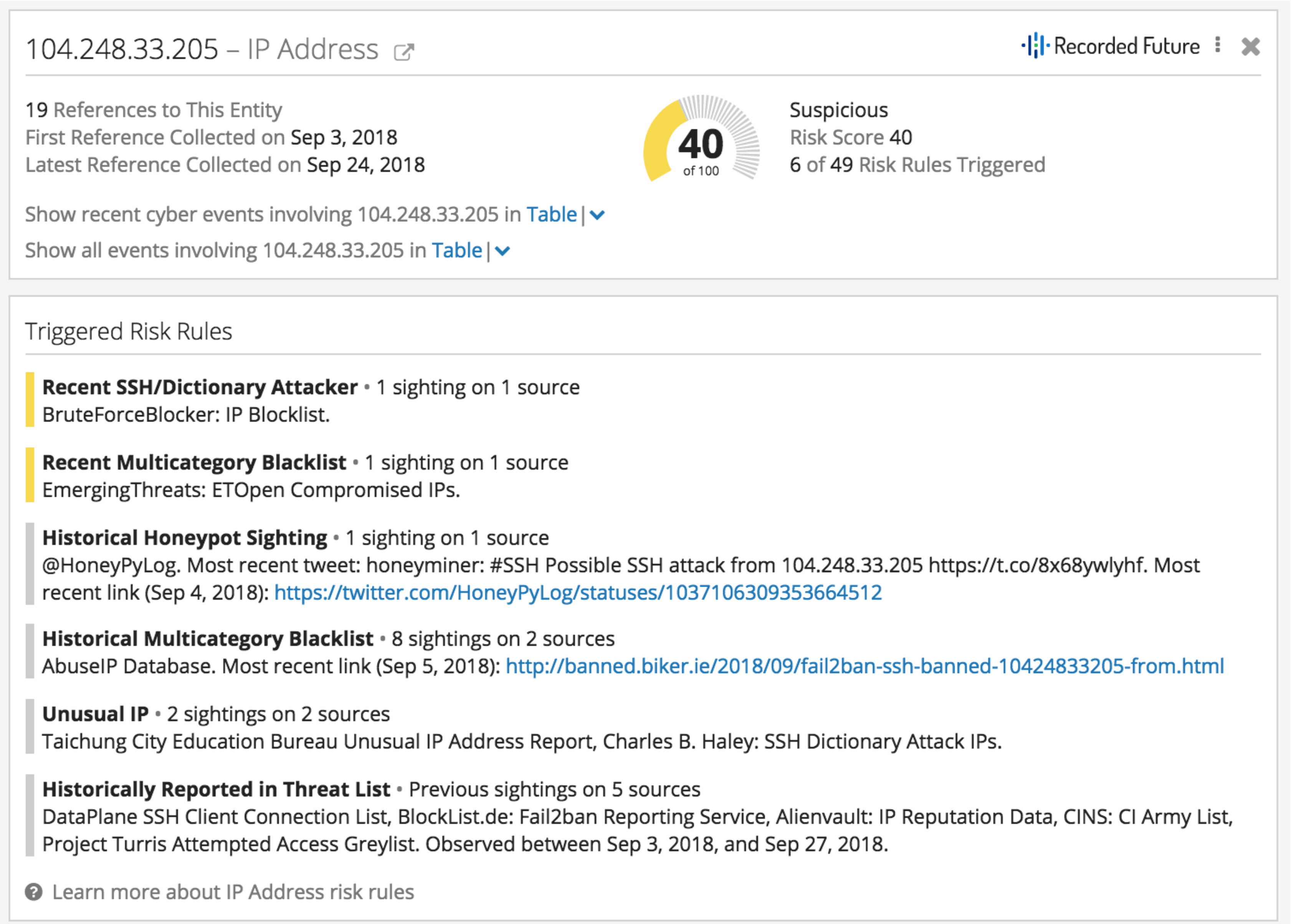
- “trend” of # unique entries with % unique
- URL, Domain data → smaller volumes, usually viewed as higher quality
- IP → known to be noisy
- Hash → reflection of sources chosen

More references can help…



IP	Severity_	iType	extracted_Source
104.248.33.205	2-High	c2_ip	[redacted]
104.248.33.205	3-Medium	scan_ip	[redacted]
104.248.33.205	3-Medium	scan_ip	[redacted]
104.248.33.205	3-Medium	scan_ip	[redacted]
104.248.33.205	4-Low	bot_ip	[redacted]
104.248.33.205	4-Low	brute_ip	[redacted]
104.248.33.205	4-Low	brute_ip	[redacted]
104.248.33.205	4-Low	brute_ip	[redacted]

…but additional context is even better



104.248.33.205 – IP Address

19 References to This Entity
First Reference Collected on Sep 3, 2018
Latest Reference Collected on Sep 24, 2018

Suspicious
Risk Score 40
6 of 49 Risk Rules Triggered

Show recent cyber events involving 104.248.33.205 in Table |

Show all events involving 104.248.33.205 in Table |

Triggered Risk Rules

Recent SSH/Dictionary Attacker • 1 sighting on 1 source
BruteForceBlocker: IP Blocklist.

Recent Multicategory Blacklist • 1 sighting on 1 source
EmergingThreats: ETOpen Compromised IPs.

Historical Honeypot Sighting • 1 sighting on 1 source
@HoneyPyLog. Most recent tweet: honeyminer: #SSH Possible SSH attack from 104.248.33.205 https://t.co/8x68ywlyhf. Most recent link (Sep 4, 2018): https://twitter.com/HoneyPyLog/statuses/1037106309353664512

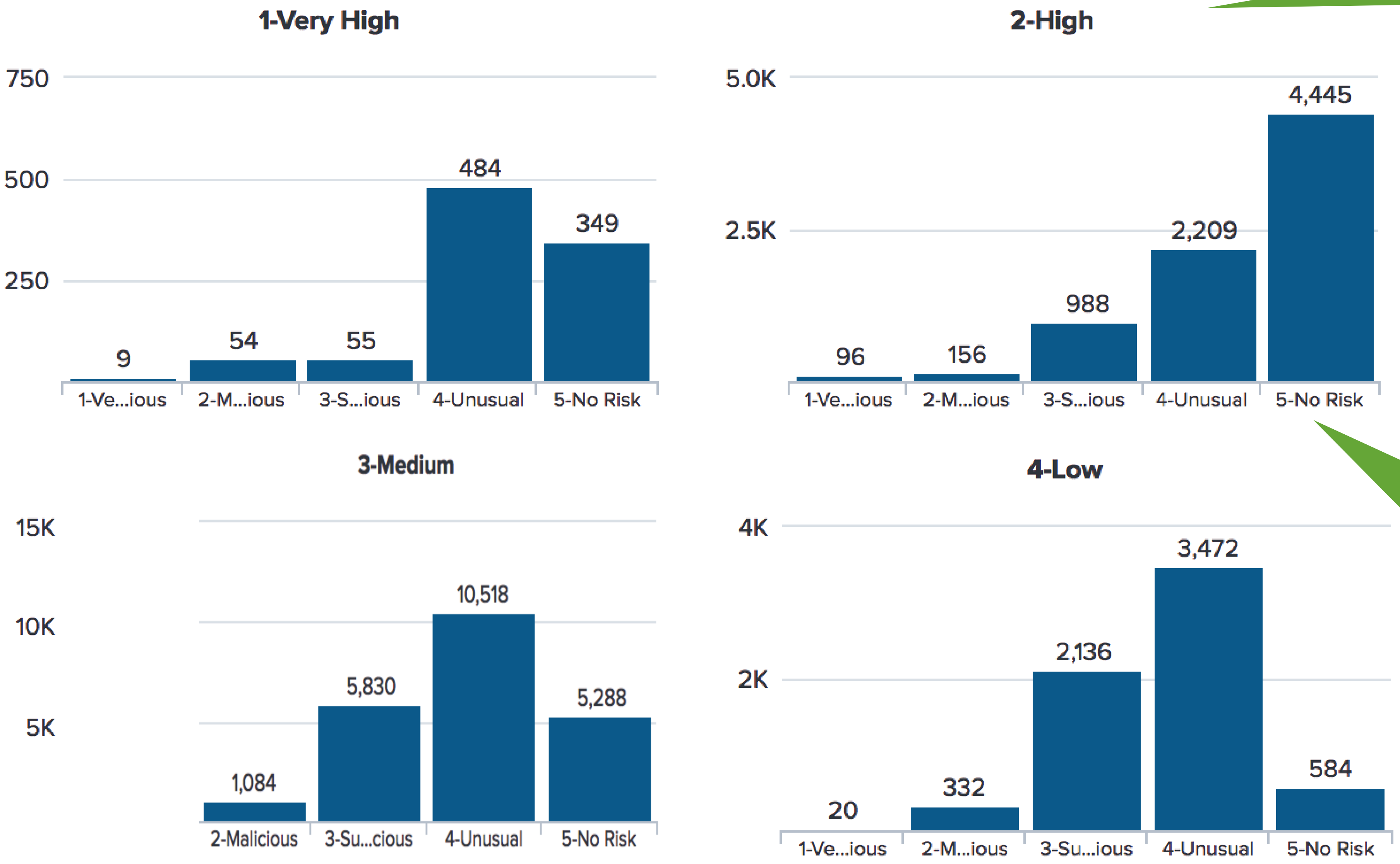
Historical Multicategory Blacklist • 8 sightings on 2 sources
AbuseIP Database. Most recent link (Sep 5, 2018): http://banned.biker.ie/2018/09/fail2ban-ssh-banned-10424833205-from.html

Unusual IP • 2 sightings on 2 sources
Taichung City Education Bureau Unusual IP Address Report, Charles B. Haley: SSH Dictionary Attack IPs.

Historically Reported in Threat List • Previous sightings on 5 sources
DataPlane SSH Client Connection List, BlockList.de: Fail2ban Reporting Service, Alienvault: IP Reputation Data, CINS: CI Army List, Project Turris Attempted Access Greylist. Observed between Sep 3, 2018, and Sep 27, 2018.

Learn more about IP Address risk rules

A collective scoring method vs GRF collection



GRF Severity

Vendor criticality (“Very Malicious”, “Malicious”, etc.)

IMPACT AND NEXT STEPS

- Data redundancy as expected
  - High priority to determine “good“ vs “bad” redundancy
- Source validity and confidence are abstract
  - Continued need to develop better scoring methods (crowd sourcing, historic reliability, source reputation)
- Direct member contributions are small % of indicators
  - ISACs/ISAOs need to find ways to simplify feedback and sharing while respecting privacy
  - Large open source dataset still needed for comparable threat landscape

Sharing with too many indicators

Our Speakers

KEN TOWNE

Director of Technology
Global Resilience Federation
ktowne@grfederation.org

GLENN WONG

Director of Product Management
Recorded Future
glenn@recordedfuture.com