



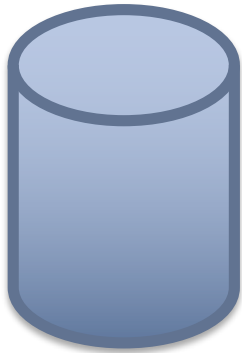
# The Carrier-Grade NAT Information Gap and Source Port Logging



Dave O'Reilly, Chief Technologist, FTR Solutions

IETF-102 OPSEC WG  
20<sup>th</sup> July 2018

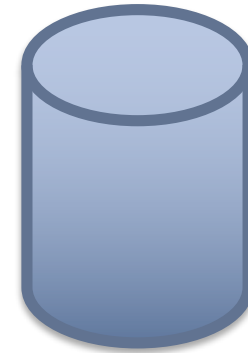
# The Problem



Victim/Service Provider Records

Suspect →

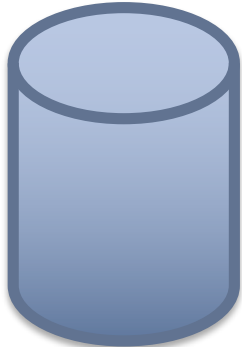
Time	IP
1	W
3	H
3	I
4	K
5	M



ISP/CGN Subscriber Database

Time	IP	Port	Subscriber
1	W	A	Bob
1	W	B	John ?
1	W	C	Liz
2	Y	D	Eric
2	Z	E	Joe

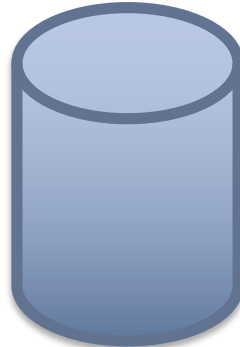
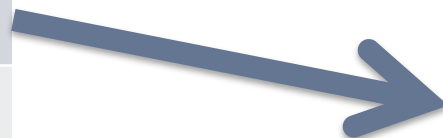
# Solution 1 of 4 – Connection Logging



Victim/Service Provider Records

Suspect →

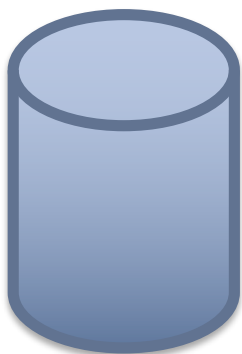
Time	IP
1	W
3	H
3	I
4	K
5	M



ISP/CGN Subscriber Database

Time	IP	Port	Dest	Subscriber
1	W	A	V	Bob
1	W	B	G	John
1	W	C	H	Liz
2	Y	D	G	Eric
2	Z	E	V	Joe

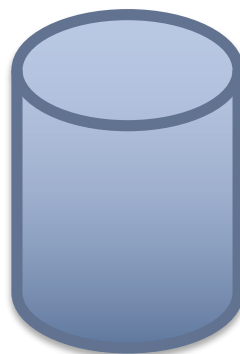
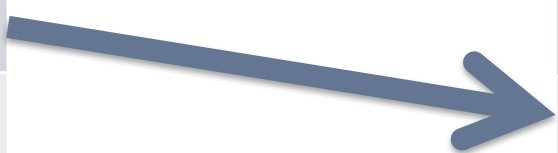
# Solution 2 of 4 – IPv6



Victim/Service Provider Records

Time	IP
1	W::Z
3	H::L
3	I::M
4	K::R
5	M::S

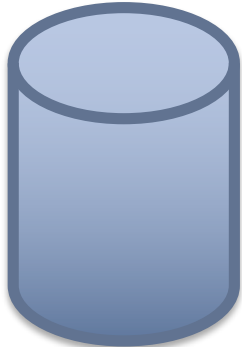
Suspect →



ISP/CGN Subscriber Database

Time	IP	Subscriber
1	W::X	Bob
1	W::Z	John
1	W::H	Liz
2	Y::G	Eric
2	Z::T	Joe

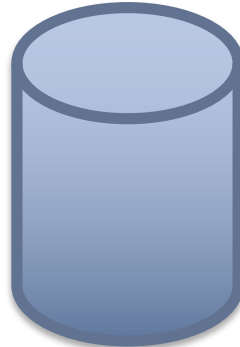
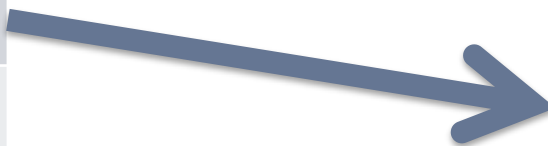
# Solution 3 of 4 – Don't use Carrier-Grade NAT



Victim/Service Provider Records

Time	IP
1	W
3	H
3	I
4	K
5	M

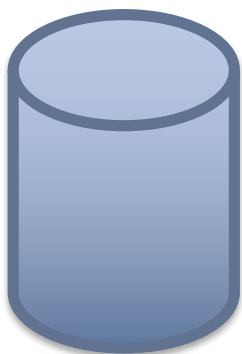
Suspect →



ISP/CGN Subscriber Database

Time	IP	Subscriber
1	W	Bob
1	W	John
1	W	Liz
2	Y	Eric
2	Z	Joe

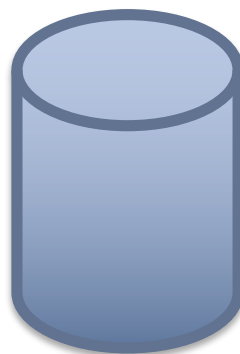
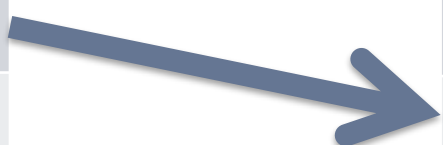
# Solution 4 of 4 – Source Port Logging



Victim/Service Provider Records

Suspect →

Time	IP	Port
1	W	B
3	H	9
3	I	8
4	K	7
5	M	6



ISP/CGN Subscriber Database

Time	IP	Port	Subscriber
1	W	A	Bob
1	W	B	John
1	W	C	Liz
2	Y	D	Eric
2	Z	E	Joe

# Log Source Port: Challenges

Awareness

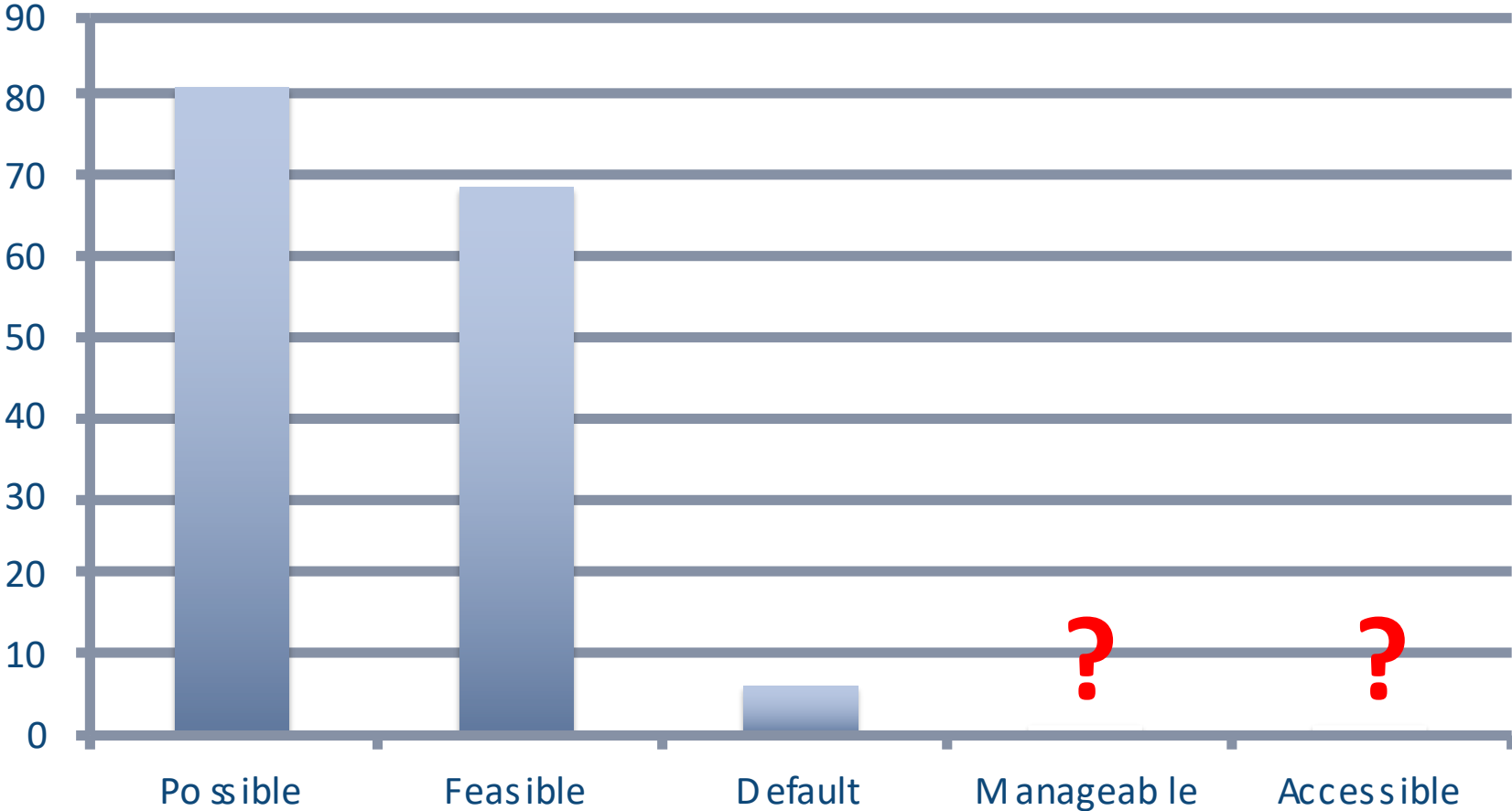
Software  
Support

Storage

Breaking  
Other Tooling

Time  
Accuracy

# Software Support





# Further Reading

**“Approaches to Address the Availability of Information in Criminal Investigations Involving Large-Scope IP Address Sharing Technologies.”**

<https://tools.ietf.org/html/draft-daveor-cgn-logging-04>

Also:

- <https://www.ftrsolutions.com/index.php/resources/carrier-grade-nat>
- <https://www.ftrsolutions.com/index.php/resources>



# Thank You! Any Questions?



Dave O'Reilly  
Chief Technologist  
FTR Solutions

+353 (87) 231 3257  
dave.oreilly@ftrsolutions.com