THREAT INTELLIGENCE SHARING: LESSONS FROM THE FRONT LINES

THAT DAY YOU BECAME A BANK

DATA IS YOUR FUTURE OR IT ISN'T

YES, YOU HAVE AN ENEMY

AND PROBABLY MORE THAN ONE

WE'RE SURROUNDED

CONSTANT COMPROMISE SIMPLIFIES THE PROBLEM

ADAPTIVE ADVERSARIES

THEY HAVE (AT LEAST) THREE THINGS YOU DON'T

HARD SECURITY TRUTH

BEST SECURITY ORGS AND TECHNOLOGIES HAVE BEEN HACKED

YOU ARE YOUR OWN POLICE

TRACKING ALL OF THE BAD GUYS IS NOW YOUR JOB

YOU NEED YET ANOTHER TOOL

FIREWALLS, IDS, ANTIMALWARE, WHITELISTING, INTEGRITY, HONEYPOT

THE HOLY GRAIL OF SECURITY

YAY! THREAT INTELLIGENCE SHARING PLATFORMS!

DON'T FORGET THE EASY STUFF

SECURITY BASICS, DEFENSE IN DEPTH AND PROCESS MATURITY

AUTOMATION FTW

ACHIEVEMENT UNLOCKED: LEVEL UP!

THREAT, DEFINED

INTENT, CAPABILITY AND OPPORTUNITY

HUMANS ARE BAD AT THIS

AND WE'RE VERY GOOD AT FORGETTING

SOME DATA IS BETTER THAN NO DATA
IN THE LAND OF THE BLIND, THE ONE EYED MAN IS KING

DATA ISN'T INTELLIGENCE

THE VALUE OF DATA IS IN THE ANALYSIS

SHARING IS CARING

VOLUNTARY VS. INVOLUNTARY

WHERE DOES YOUR INTEL GO?

BOATS, THE BORG, AND BLACK HOLES

SIZE MATTERS

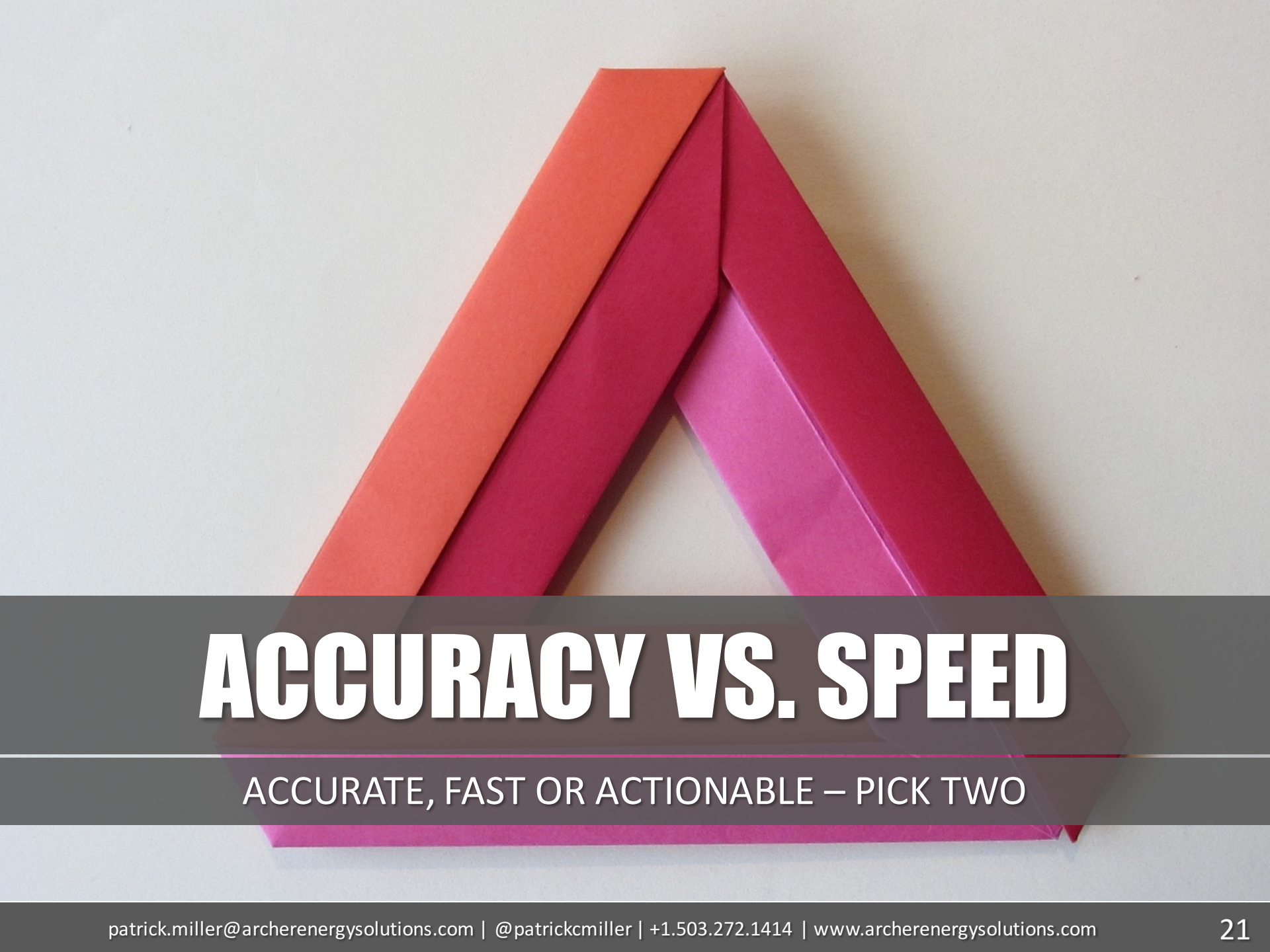
VALUE OF INFO IS INVERSELY PROPORTIONAL TO DISTRIBUTION

NEED TO KNOW BASIS

INTENT, ACCIDENT, DATA ENTROPY AND MURPHY'S LAW

ONE RING TO RULE THEM ALL

CLEARINGHOUSE VS. VIRAL



ACCURACY VS. SPEED

ACCURATE, FAST OR ACTIONABLE – PICK TWO

MEASUREMENT RULES

START MEASURING, THEN START OVER. LATHER RINSE REPEAT.

GET CONNECTED

RELATIONSHIPS + TRUST = SHARING

CHOOSE YOUR PATH

MONEY, TIME, RESOURCES AND THE ASYMPTOTIC CURVE

CREDITS

Slide 1 – HTTPS://FLIC.KR/P/M71BMQ
Slide 2 – HTTPS://FLIC.KR/P/BHGNWK
Slide 3 – HTTPS://FLIC.KR/P/4RK9E4
Slide 4 – HTTPS://FLIC.KR/P/7X5PJK
Slide 5 – HTTPS://FLIC.KR/P/QKTEJU
Slide 6 – HTTPS://FLIC.KR/P/5PZ1UJ
Slide 7 – HTTPS://FLIC.KR/P/7CUNJ8
Slide 8 – HTTPS://GOO.GL/WDPQQ
Slide 9 – HTTPS://FLIC.KR/P/73QDMF
Slide 10 – HTTPS://FLIC.KR/P/ARXDVK
Slide 11 – HTTPS://FLIC.KR/P/STAA
Slide 12 – HTTPS://FLIC.KR/P/OKNKRP
Slide 13 – HTTPS://FLIC.KR/P/7OY8XK
Slide 14 – HTTPS://FLIC.KR/P/2B1JP
Slide 15 – HTTPS://FLIC.KR/P/6WPMV
Slide 16 – HTTPS://FLIC.KR/P/7YVSZP
Slide 17 – HTTPS://FLIC.KR/P/QTYGZF
Slide 18 – HTTPS://FLIC.KR/P/3ERYGD
Slide 19 – HTTPS://FLIC.KR/P/65HWNW
Slide 20 – HTTPS://FLIC.KR/P/9PQHY4
Slide 21 – HTTPS://FLIC.KR/P/RWJESY
Slide 22 – HTTPS://FLIC.KR/P/PKXHAR
Slide 23 – HTTPS://FLIC.KR/P/8VWTHD
Slide 24 – HTTPS://FLIC.KR/P/EAUJHV

PATRICK C MILLER

CRISC CISA CISSP-ISSAP SSCP CEH NSA-IAM CVI
Managing Partner, Archer Energy Solutions
patrick.miller@archerenergysolutions.com
@patrickcmiller
+1 503.272.1414