Converging Behaviors Across Threat Actors

Joe Slowik, Paralus LLC

Quick Background

- *Current:*
  - *CTI & ICS/OT Consulting @ Paralus LLC*
  - *Threat Intelligence Management @ Huntress*
- *Previous:*
  - *Threat Intelligence & Detection Engineering Lead @ Gigamon*
  - *Threat Research @ DomainTools & Dragos*
  - *Incident Response Lead @ Los Alamos National Laboratory*
  - *“Various” @ US Navy*

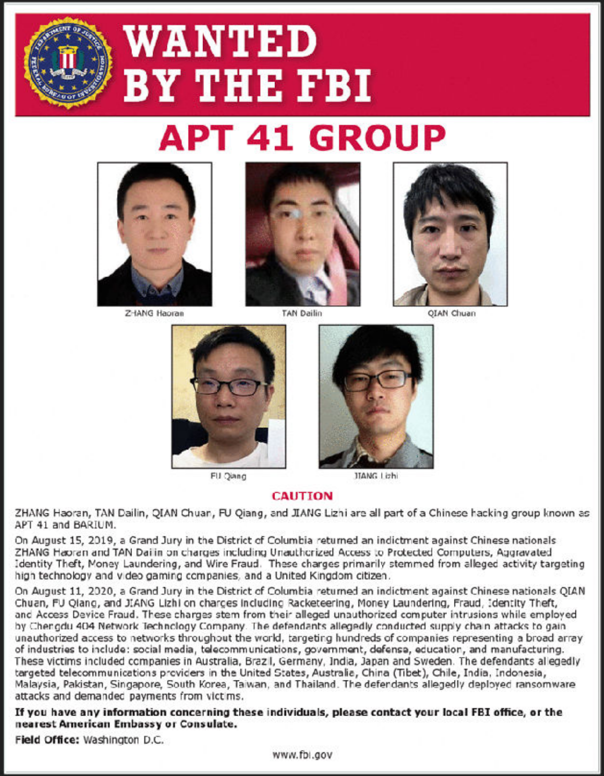
Agenda

- Defining Adversaries
- The Relationship Between Operations & Tools
- Implications Of Convergence
- Conclusions

Defining “Adversaries”

Defining Adversaries

Defining Adversaries



WANTED BY THE FBI

APT 41 GROUP

ZHANG Haoran

TAN Dailin

QIAN Chuan

FU Qiang

JIANG Lizhi

CAUTION

ZHANG Haoran, TAN Dailin, QIAN Chuan, FU Qiang, and JIANG Lizhi are all part of a Chinese hacking group known as APT 41 and BARIUM.

On August 15, 2019, a Grand Jury in the District of Columbia returned an indictment against Chinese nationals ZHANG Haoran and TAN Dailin on charges including Unauthorized Access to Protected Computers, Aggravated Identity Theft, Money Laundering, and Wire Fraud. These charges primarily stemmed from alleged activity targeting high technology and video gaming companies, and a United Kingdom citizen.

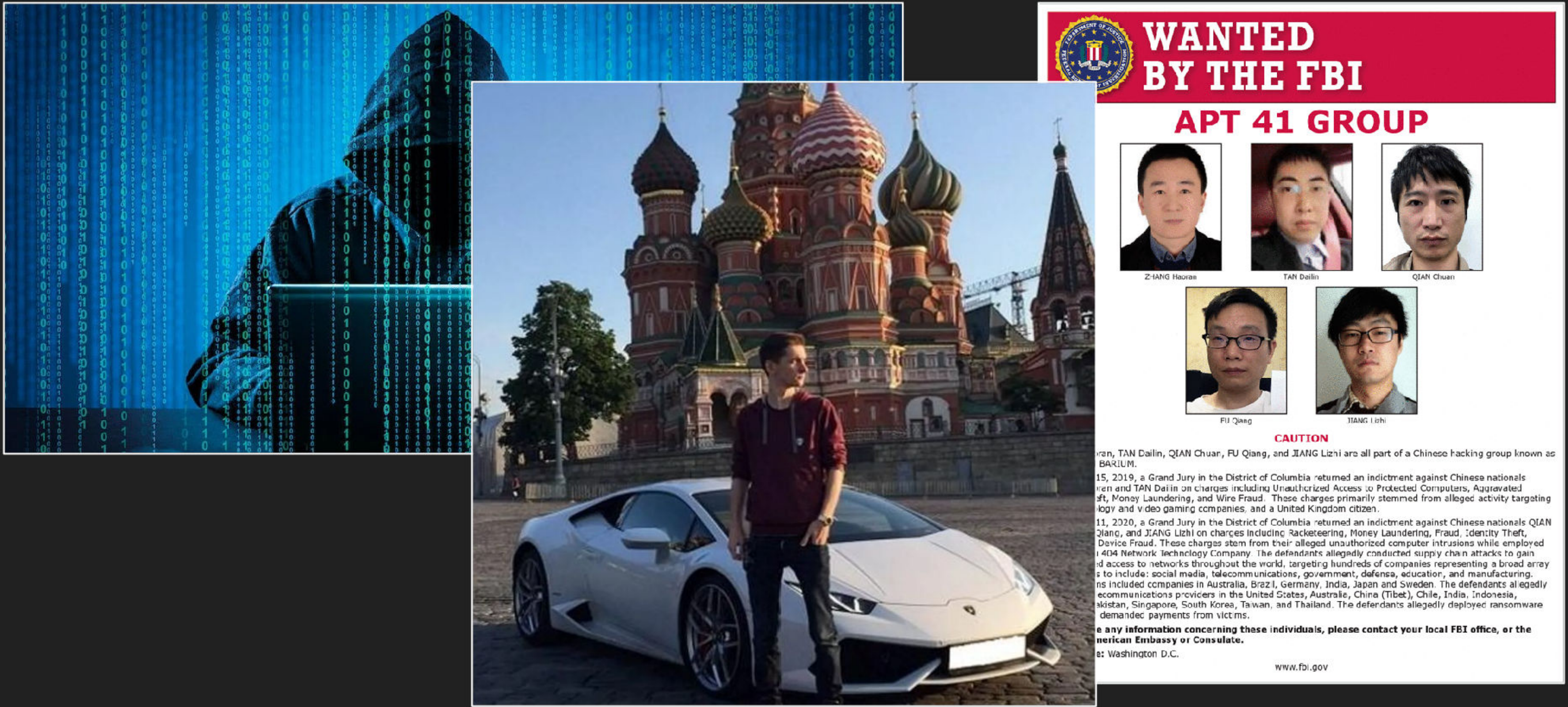
On August 11, 2020, a Grand Jury in the District of Columbia returned an indictment against Chinese nationals QIAN Chuan, FU Qiang, and JIANG Lizhi on charges including Racketeering, Money Laundering, Fraud, Identity Theft, and Access Device Fraud. These charges stem from their alleged unauthorized computer intrusions while employed by Chengdu 404 Network Technology Company. The defendants allegedly conducted supply chain attacks to gain unauthorized access to networks throughout the world, targeting hundreds of companies representing a broad array of industries to include: social media, telecommunications, government, defense, education, and manufacturing. These victims included companies in Australia, Brazil, Germany, India, Japan and Sweden. The defendants allegedly targeted telecommunications providers in the United States, Australia, China (Tibet), Chile, India, Indonesia, Malaysia, Pakistan, Singapore, South Korea, Taiwan, and Thailand. The defendants allegedly deployed ransomware attacks and demanded payments from victims.

If you have any information concerning these individuals, please contact your local FBI office, or the nearest American Embassy or Consulate.

Field Office: Washington D.C.

www.fbi.gov

Defining Adversaries



WANTED BY THE FBI

APT 41 GROUP

ZHANG Haoran

TAN Dailin

QIAN Chuan

FU Qiang

JIANG Lizhi

CAUTION

oran, TAN Dailin, QIAN Chuan, FU Qiang, and JIANG Lizhi are all part of a Chinese hacking group known as BARIUM.

15, 2019, a Grand Jury in the District of Columbia returned an indictment against Chinese nationals oran and TAN Dailin on charges including Unauthorized Access to Protected Computers, Aggravated eft, Money Laundering, and Wire Fraud. These charges primarily stemmed from alleged activity targeting ology and video gaming companies, and a United Kingdom citizen.

11, 2020, a Grand Jury in the District of Columbia returned an indictment against Chinese nationals QIAN Qiang, and JIANG Lizhi on charges including Racketeering, Money Laundering, Fraud, Identity Theft, Device Fraud. These charges stem from their alleged unauthorized computer intrusions while employed 404 Network Technology Company. The defendants allegedly conducted supply chain attacks to gain ed access to networks throughout the world, targeting hundreds of companies representing a broad array s to include: social media, telecommunications, government, defense, education, and manufacturing. ns included companies in Australia, Brazil, Germany, India, Japan and Sweden. The defendants allegedly ecommunications providers in the United States, Australia, China (Tibet), Chile, India, Indonesia, akistan, Singapore, South Korea, Taiwan, and Thailand. The defendants allegedly deployed ransomware demanded payments from victims.

e any information concerning these individuals, please contact your local FBI office, or the nerican Embassy or Consulate.

e: Washington D.C.

www.fbi.gov

Defining Adversaries

CHOOSE YOUR HACKER
1
RUSSIA
CHINA
NORTH KOREA
IRAN
USA
CREDITS: 0

WANTED
BY THE FBI

APT 41 GROUP

ANG Haoran
TAN Dailin
QIAN Chuan
FU Qiang
JIANG Lizhi

CAUTION

in, QIAN Chuan, FU Qiang, and JIANG Lizhi are all part of a Chinese hacking group known as

rand Jury in the District of Columbia returned an indictment against Chinese nationals
Dailin on charges including Unauthorized Access to Protected Computers, Aggravated
undering, and Wire Fraud. These charges primarily stemmed from alleged activity targeting
o gaming companies, and a United Kingdom citizen.

rand Jury in the District of Columbia returned an indictment against Chinese nationals QIAN
ANG Lizhi on charges including Racketeering, Money Laundering, Fraud, Identity Theft,
. These charges stem from their alleged unauthorized computer intrusions while employed
Technology Company. The defendants allegedly conducted supply chain attacks to gain
etworks throughout the world, targeting hundreds of companies representing a broad array
ocial media, telecommunications, government, defense, education, and manufacturing.
mpanies in Australia, Brazil, Germany, India, Japan and Sweden. The defendants allegedly
ions providers in the United States, Australia, China (Tibet), Chile, India, Indonesia,
pore, South Korea, Taiwan, and Thailand. The defendants allegedly deployed ransomware
ayments from victims.

**ation concerning these individuals, please contact your local FBI office, or the
assy or Consulate.**

D.C.

www.fbi.gov

REALLY Defining Adversaries

“Person, group, organization, or government that conducts or has the intent to conduct detrimental activities.” - NIST

Conception Of Adversaries

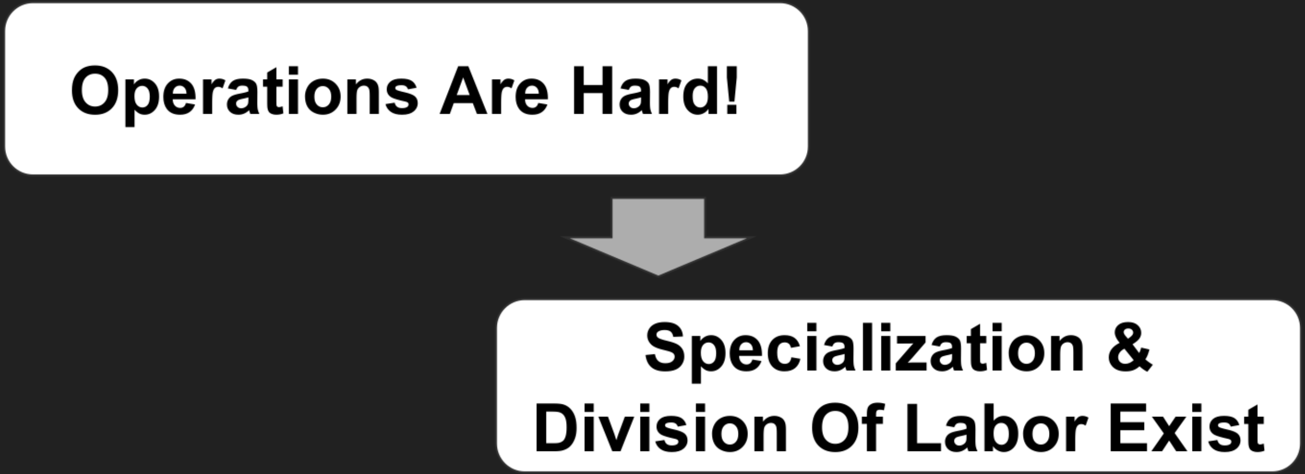
- Unitary In Nature
- Unique In Operations & Behaviors
- Readily Distinguishable From Other Adversaries

Adversary Reality

Adversary Reality

Operations Are Hard!

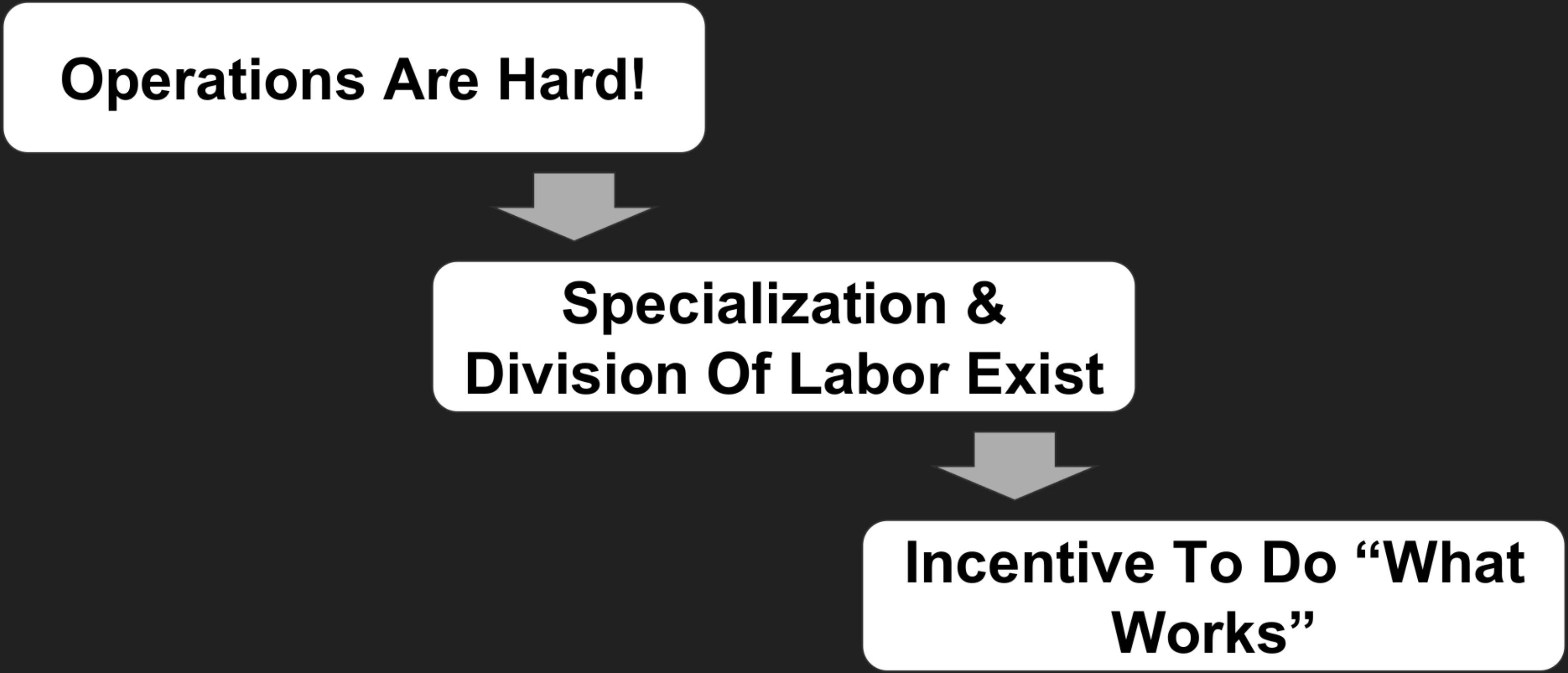
Adversary Reality



Operations Are Hard!

Specialization & Division Of Labor Exist

Adversary Reality



Operations Are Hard!

Specialization & Division Of Labor Exist

Incentive To Do “What Works”

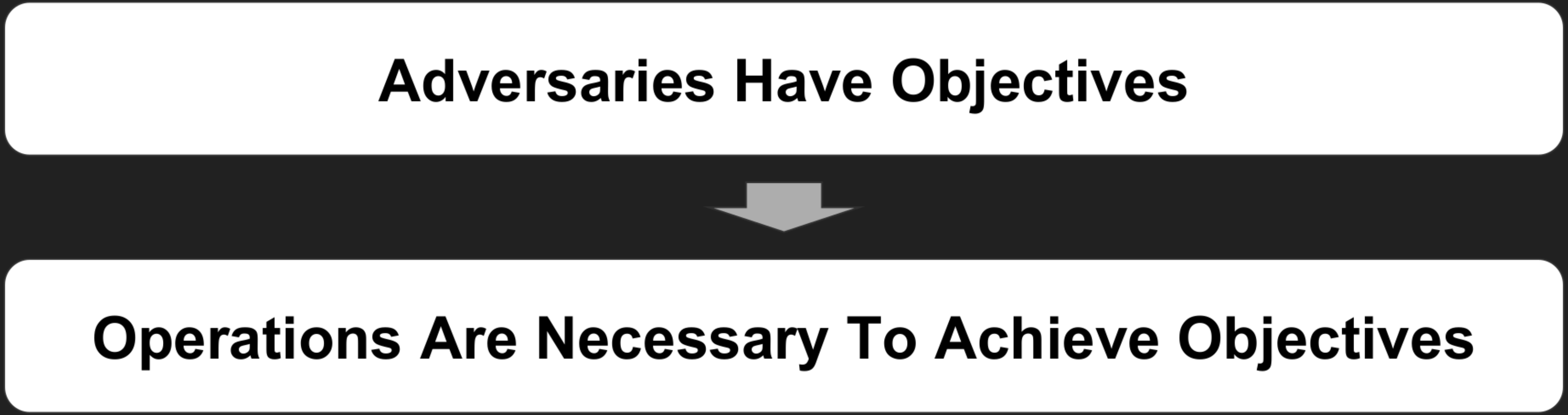
Operations & Tools

Adversaries, Ops, & Tools

Adversaries, Ops, & Tools

Adversaries Have Objectives

Adversaries, Ops, & Tools



Adversaries Have Objectives

Operations Are Necessary To Achieve Objectives

Adversaries, Ops, & Tools

Adversaries Have Objectives

Operations Are Necessary To Achieve Objectives

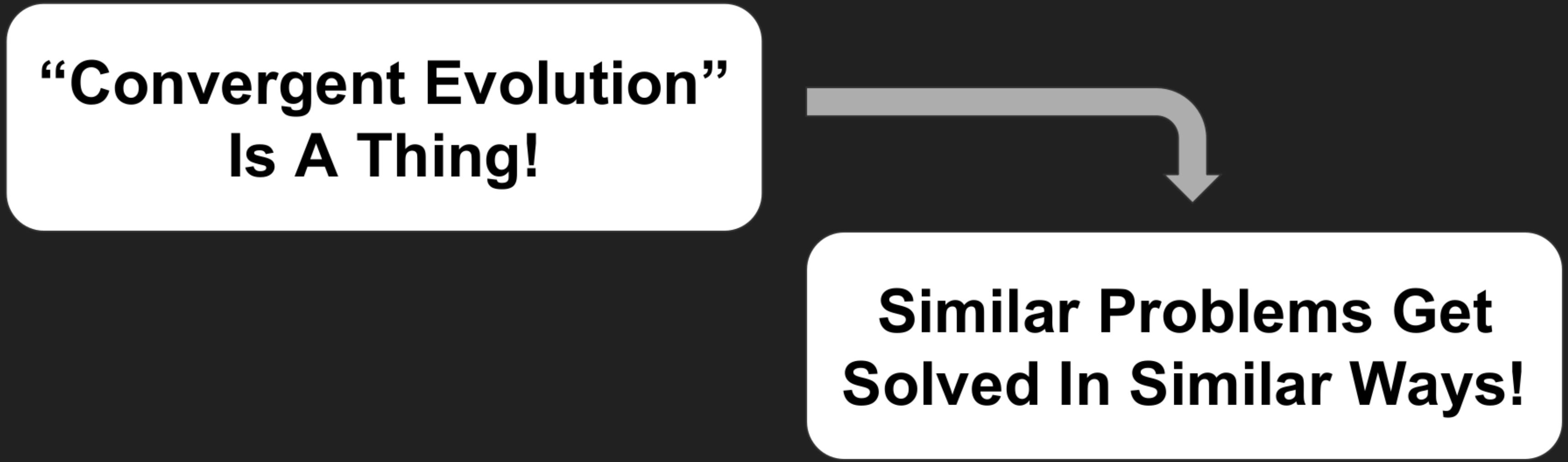
Tools Are Used To Complete Operations

Digression - Evolution!

Digression - Evolution!

“Convergent Evolution” Is A Thing!

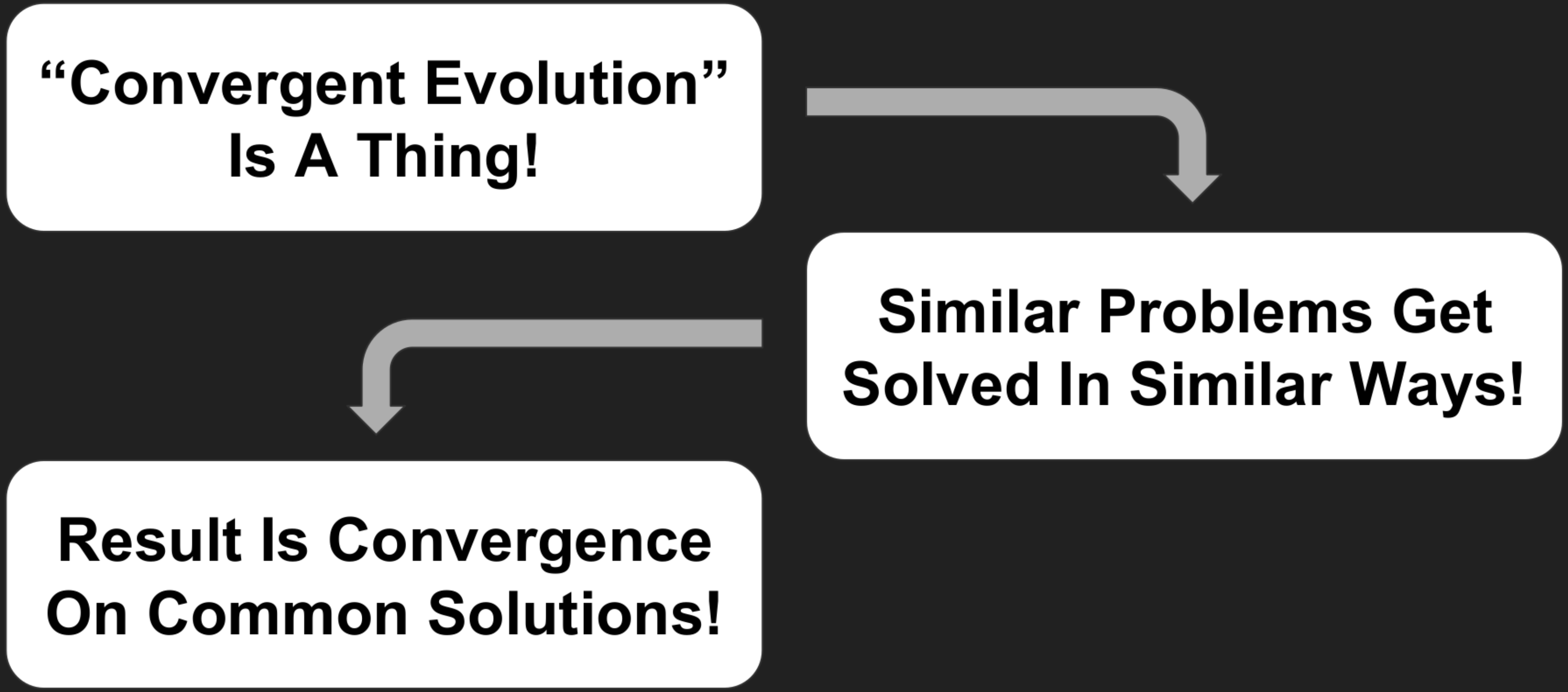
Digression - Evolution!



"Convergent Evolution" Is A Thing!

Similar Problems Get Solved In Similar Ways!

Digression - Evolution!



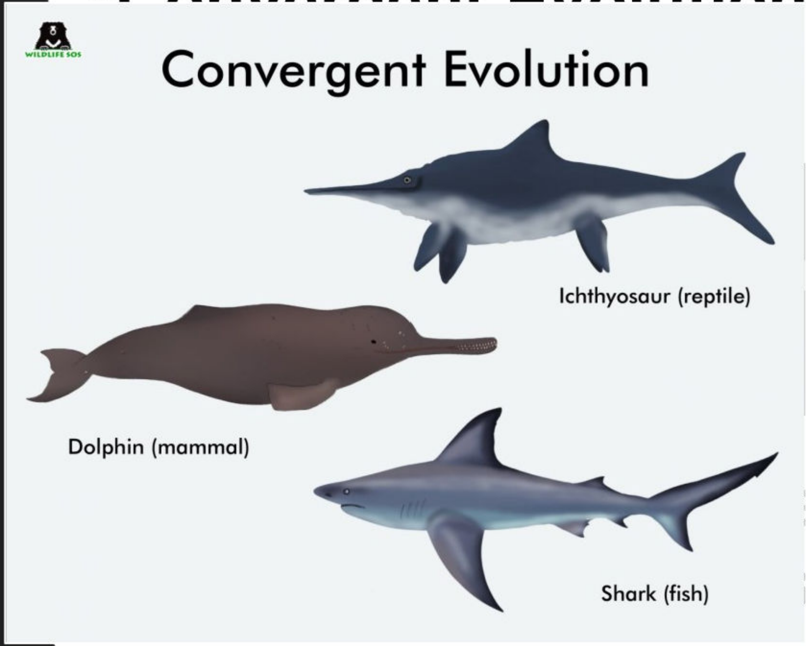
“Convergent Evolution” Is A Thing!

Similar Problems Get Solved In Similar Ways!

Result Is Convergence On Common Solutions!

Digression - Evolution!

“Convergent Evolution”



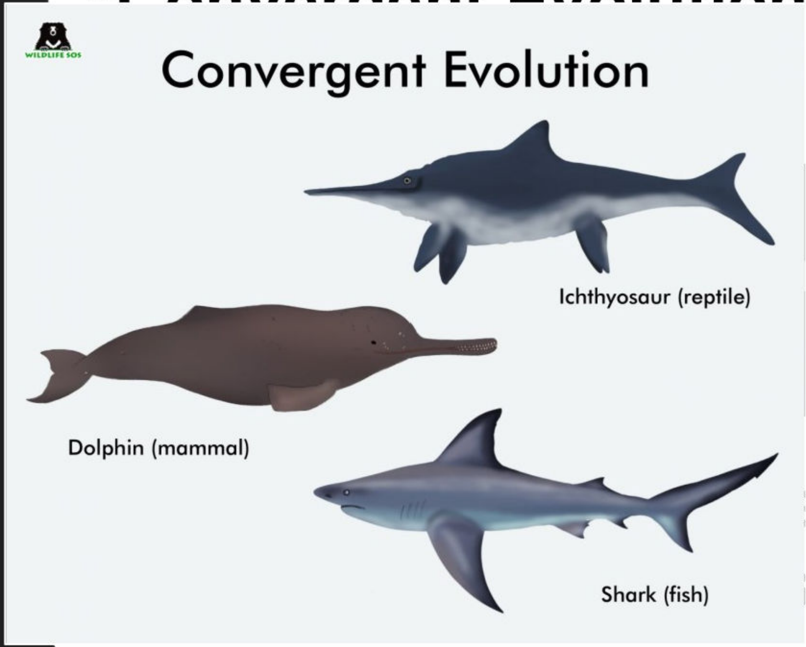
e

s!

Similar Problems Get Solved In Similar Ways!

Digression - Evolution!

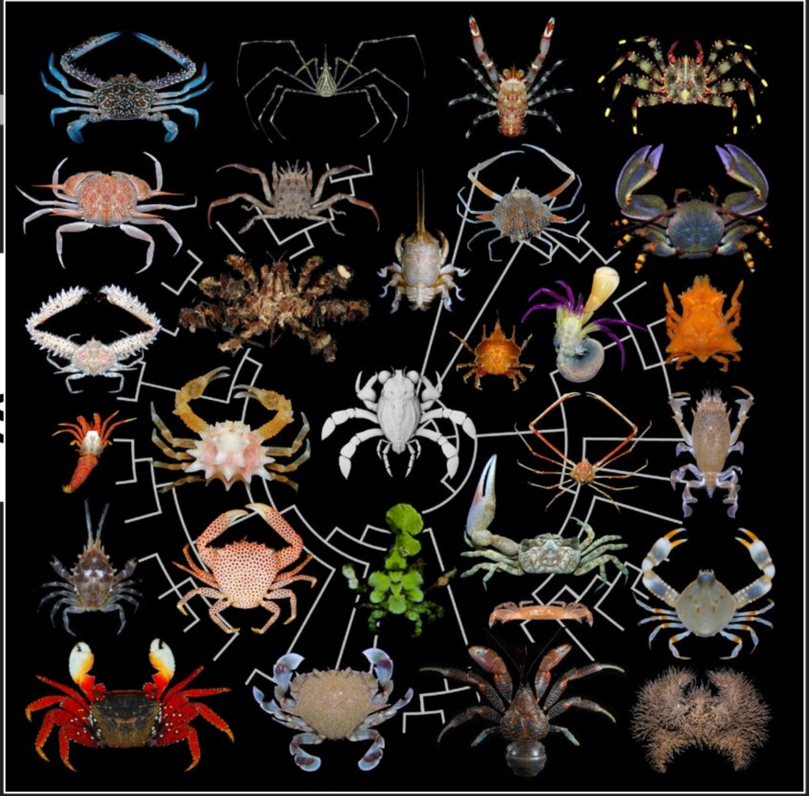
“Convergent Evolution”



S

e

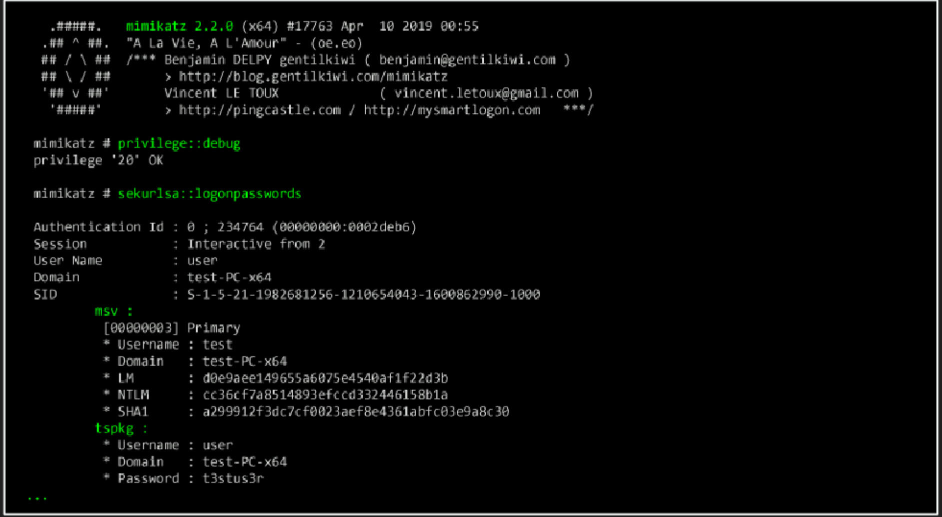
s!



Ops, Tools, & Objectives

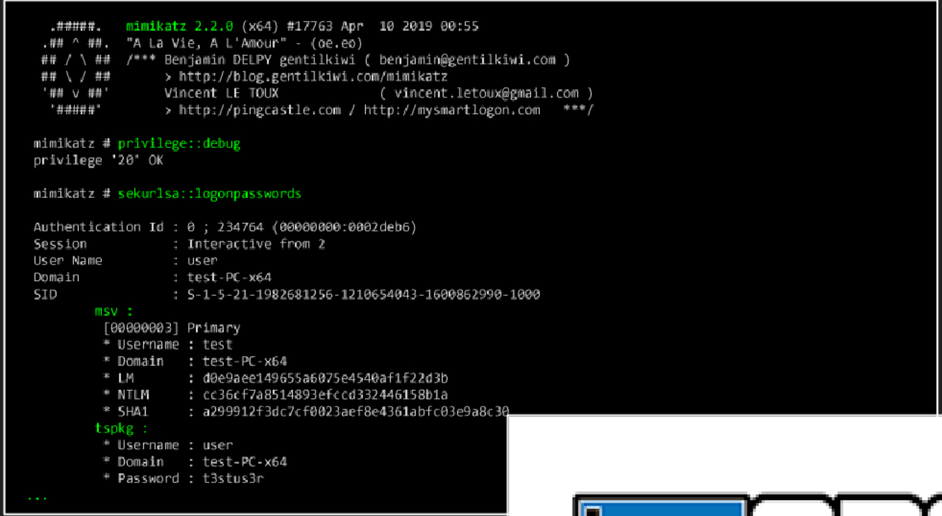
Success Is In Achieving Objectives & Mission - Not How You Got There!

Tools Of The Trade



```
  .#####.   mimikatz 2.2.0 (x64) #17763 Apr  10 2019 00:55
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY gentilkiwi ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # privilege::debug
privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 234764 (00000000:0002deb6)
Session           : Interactive from 2
User Name         : user
Domain            : test-PC-x64
SID               : S-1-5-21-1982681256-1210654043-1600862990-1000
        msv :
         [00000003] Primary
         * Username : test
         * Domain   : test-PC-x64
         * LM       : d0e9aee149655a6075e4540af1f22d3b
         * NTLM     : cc36cf7a8514893efccd332446158b1a
         * SHA1     : a299912f3dc7cf0023aef8e4361abfc03e9a8c30
        tspkg :
         * Username : user
         * Domain   : test-PC-x64
         * Password : t3stus3r
...
```

Tools Of The Trade

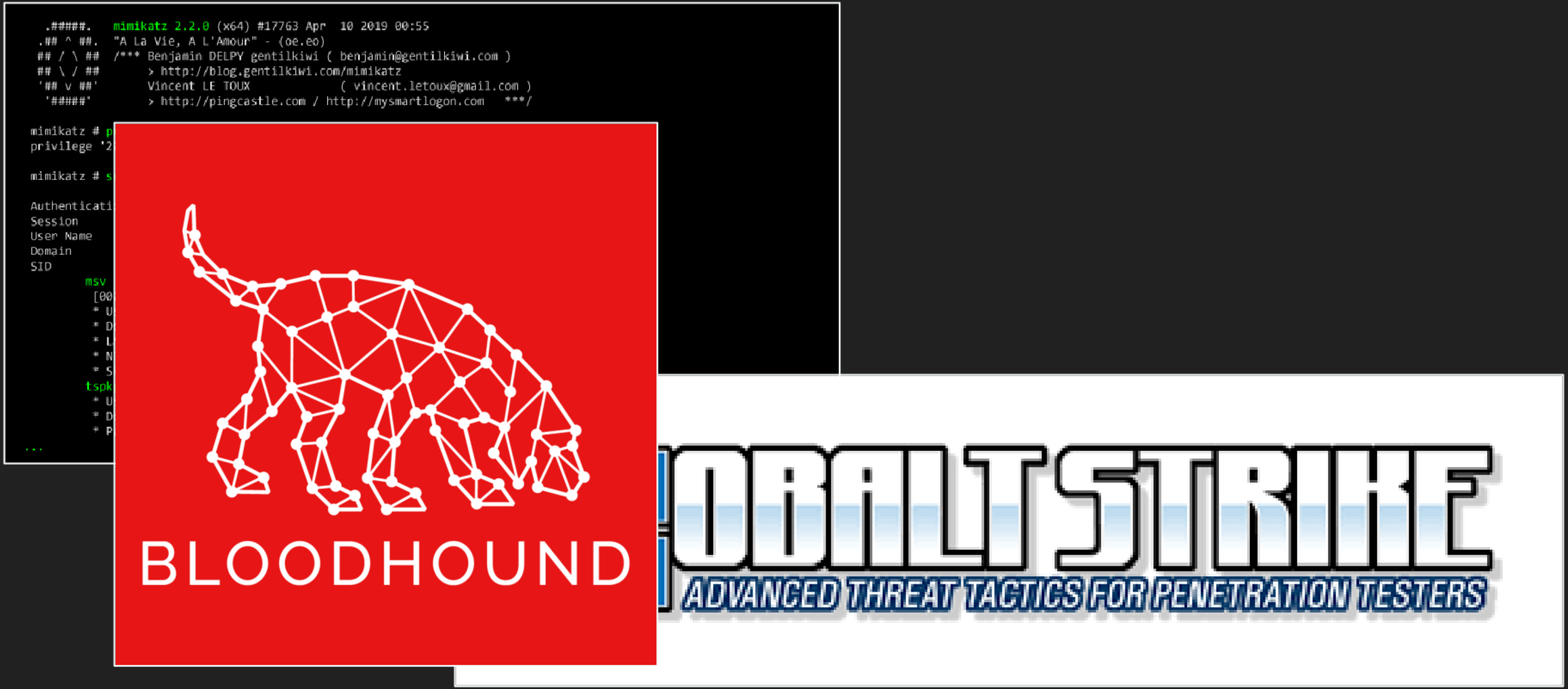


```
  .#####.   mimikatz 2.2.0 (x64) #17763 Apr  10 2019 00:55
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY gentilkiwi ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # privilege::debug
privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 234764 (00000000:0002deb6)
Session           : Interactive from 2
User Name         : user
Domain            : test-PC-x64
SID               : S-1-5-21-1982681256-1210654043-1600862990-1000
        msv :
         [00000003] Primary
         * Username : test
         * Domain   : test-PC-x64
         * LM       : d0e9aee149655a6075e4540af1f22d3b
         * NTLM     : cc36cf7a8514893efccd332446158b1a
         * SHA1     : a299912f3dc7cf0023aef8e4361abfc03e9a8c30
        tspkg :
         * Username : user
         * Domain   : test-PC-x64
         * Password : t3stus3r
...
```

COBALT STRIKE

ADVANCED THREAT TACTICS FOR PENETRATION TESTERS

Tools Of The Trade



```
  .#####.   mimikatz 2.2.0 (x64) #17763 Apr  10 2019 00:55
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY gentilkiwi ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # p
privilege '2

mimikatz # s

Authenticati
Session
User Name
Domain
SID
        msv
         [00
         * U
         * D
         * L
         * N
         * S
        tspk
         * U
         * D
         * P
...
```

Tools Of The Trade

```
  .#####.   mimikatz 2.2.0 (x64) #17763 Apr  10 2019 00:55
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY gentilkiwi ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # p
privilege '2

mimikatz # s

Authenticati
Session
User Name
Domain
SID
        msv
         [00
         * U
         * D
         * L
         * N
         * S
        tspk
         * U
         * D
         * P
 ...
```

Dying Customization

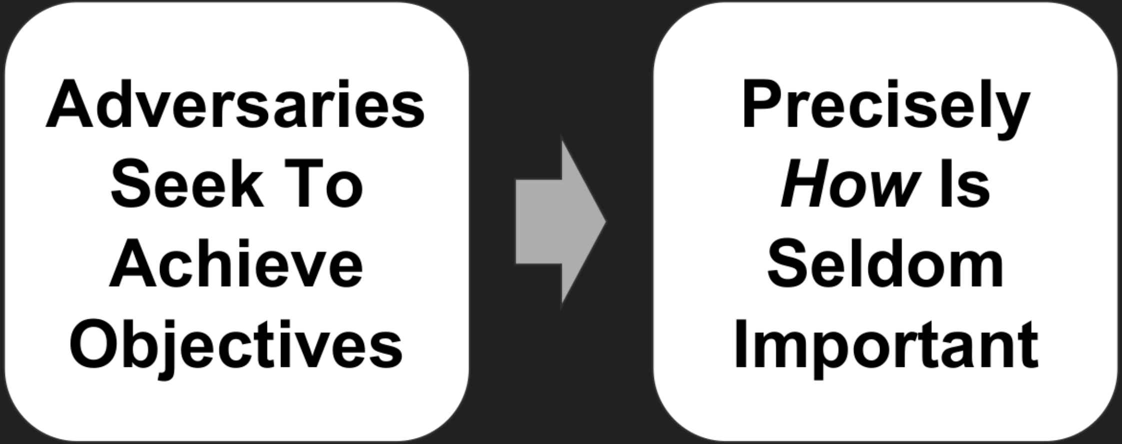
Custom Tools & Specific Capabilities Still Exist, But Have Moved To Niche Applications (ICS) Or Reserved For Special Operations (SUNBURST)

Coevolution Results

Coevolution Results

Adversaries Seek To Achieve Objectives

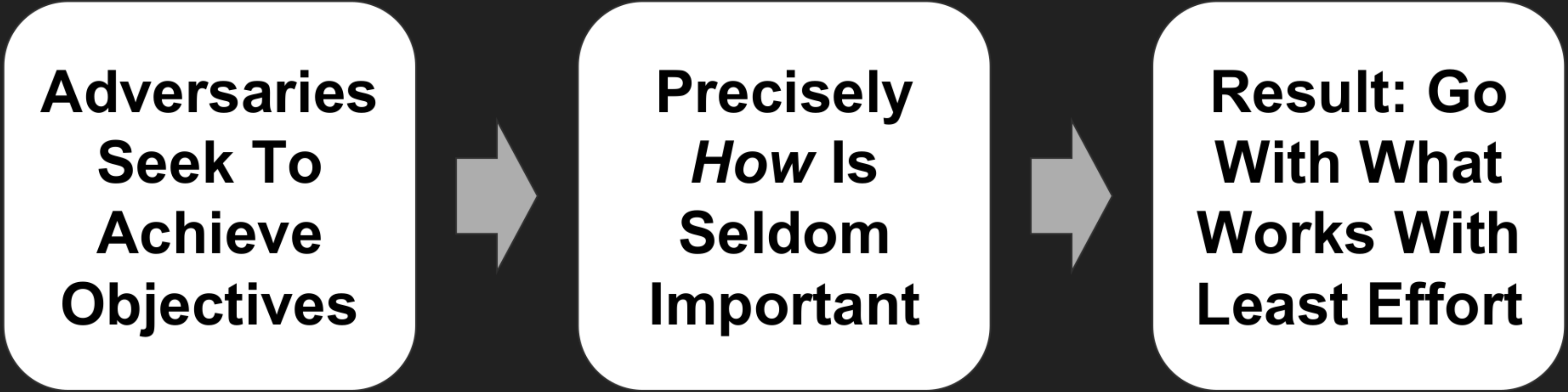
Coevolution Results



Adversaries Seek To Achieve Objectives

Precisely *How* Is Seldom Important

Coevolution Results



Adversaries Seek To Achieve Objectives

Precisely *How* Is Seldom Important

Result: Go With What Works With Least Effort

The Implications Of Convergence

What Does Convergence Mean?

Attribution Implications

Policy Effects

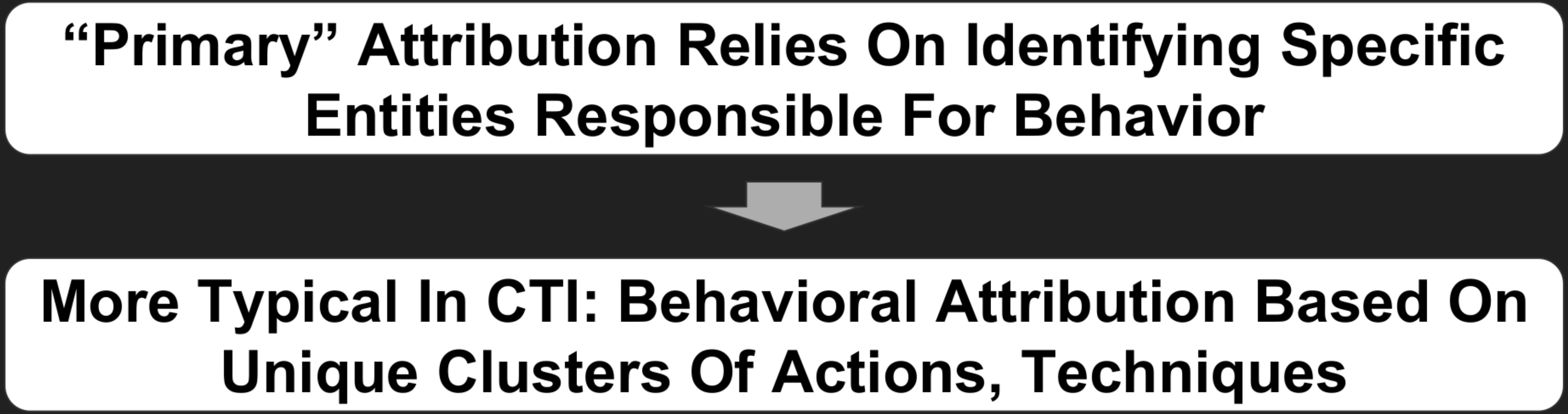
Impacts On Defense

The Question Of “Attribution”

The Question Of “Attribution”

“Primary” Attribution Relies On Identifying Specific Entities Responsible For Behavior

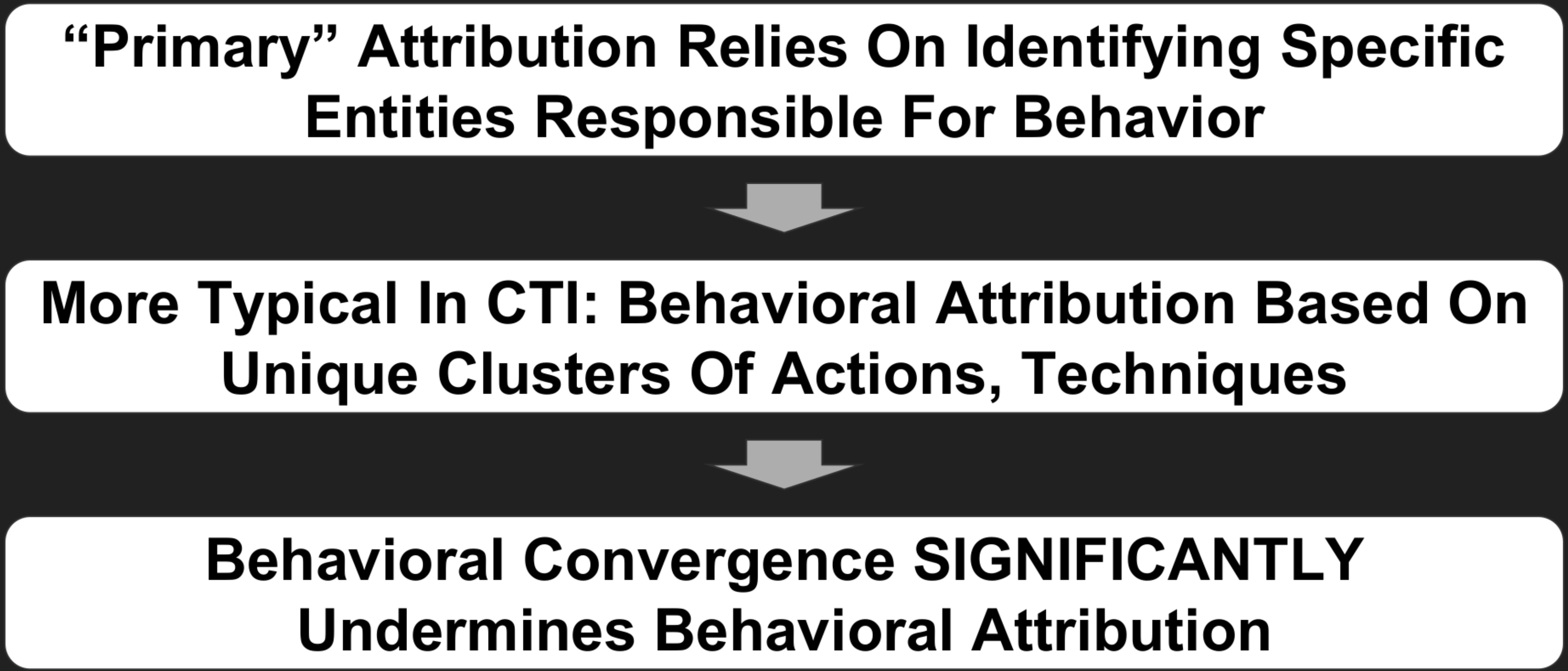
The Question Of “Attribution”



“Primary” Attribution Relies On Identifying Specific Entities Responsible For Behavior

More Typical In CTI: Behavioral Attribution Based On Unique Clusters Of Actions, Techniques

The Question Of “Attribution”



“Primary” Attribution Relies On Identifying Specific Entities Responsible For Behavior

More Typical In CTI: Behavioral Attribution Based On Unique Clusters Of Actions, Techniques

Behavioral Convergence SIGNIFICANTLY Undermines Behavioral Attribution

Attribution Impacts

Behavioral Attribution Becomes More Difficult, Clusters Overlap. May Require More Work, Resources, & Analysis To Pursue More "Formal" Attribution Types To Differentiate Adversaries!

Implications For Defense

Implications For Defense

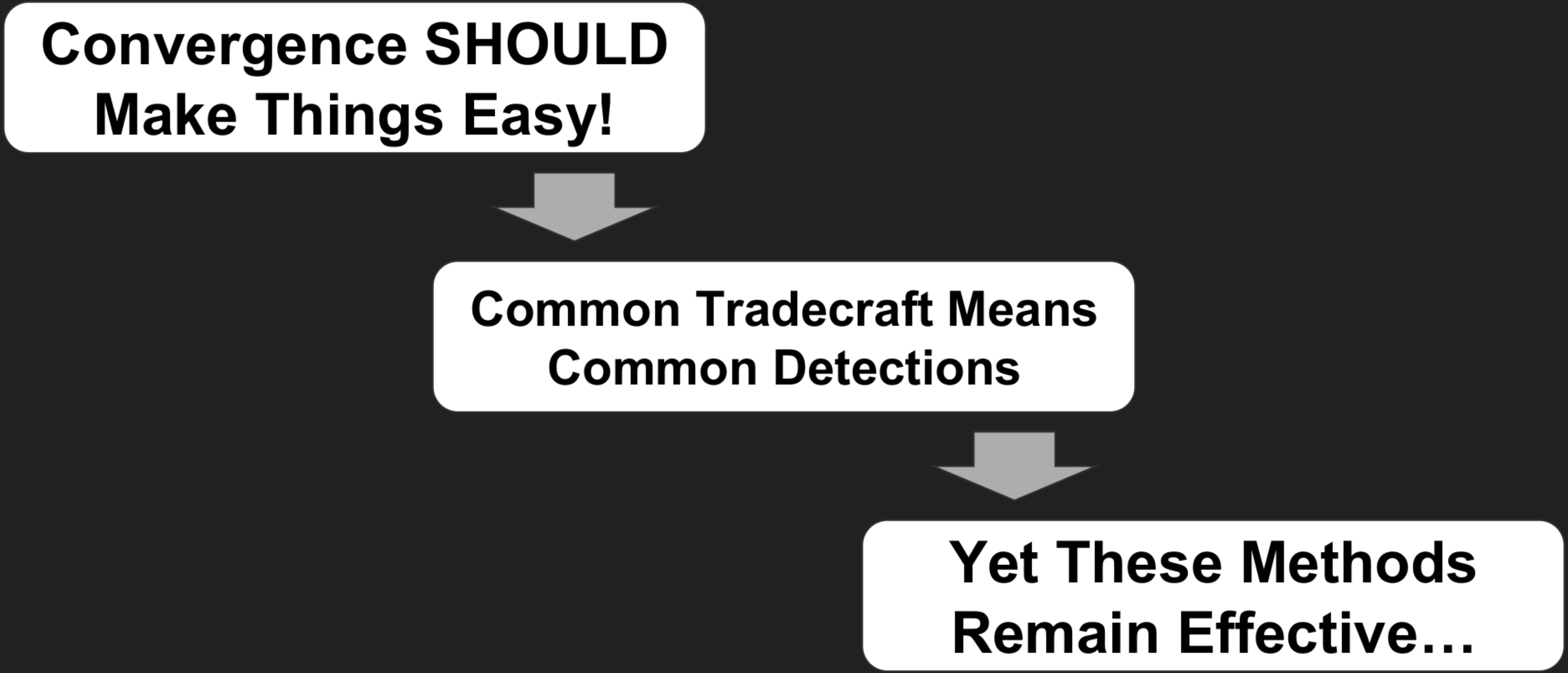
Convergence SHOULD Make Things Easy!

Implications For Defense

Convergence SHOULD Make Things Easy!

Common Tradecraft Means Common Detections

Implications For Defense



Convergence SHOULD Make Things Easy!

Common Tradecraft Means Common Detections

Yet These Methods Remain Effective…

Improving Defense

Adversaries Converge On Tradecraft Because It WORKS - Defenders Can’t Rely On Indicator Or Specific Identifiers Of Threats Anymore!

Improving Defense

Adversaries Converge On Tradecraft Because It WORKS - Defenders Can't Rely On Indicator Or Specific Identifiers Of Threats Anymore!

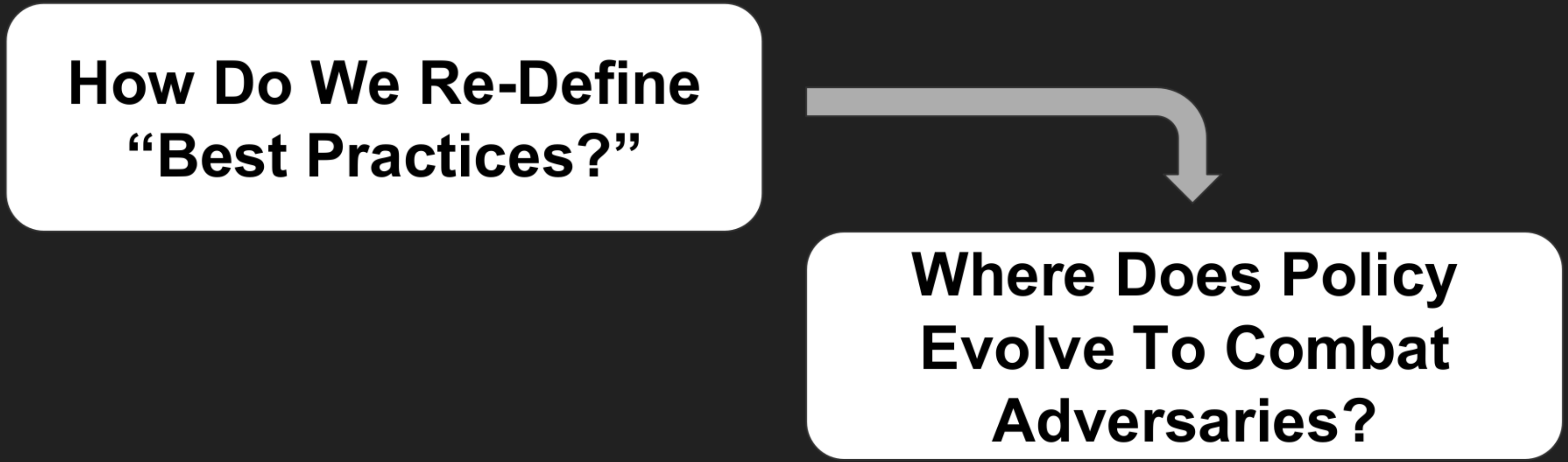
Defenders Must Migrate Toward Behavior-Centric Detectors, Anomaly Detection, & Identifying Malicious Use Of Benign Tools!

Policy Concerns

Policy Concerns

How Do We Re-Define “Best Practices?”

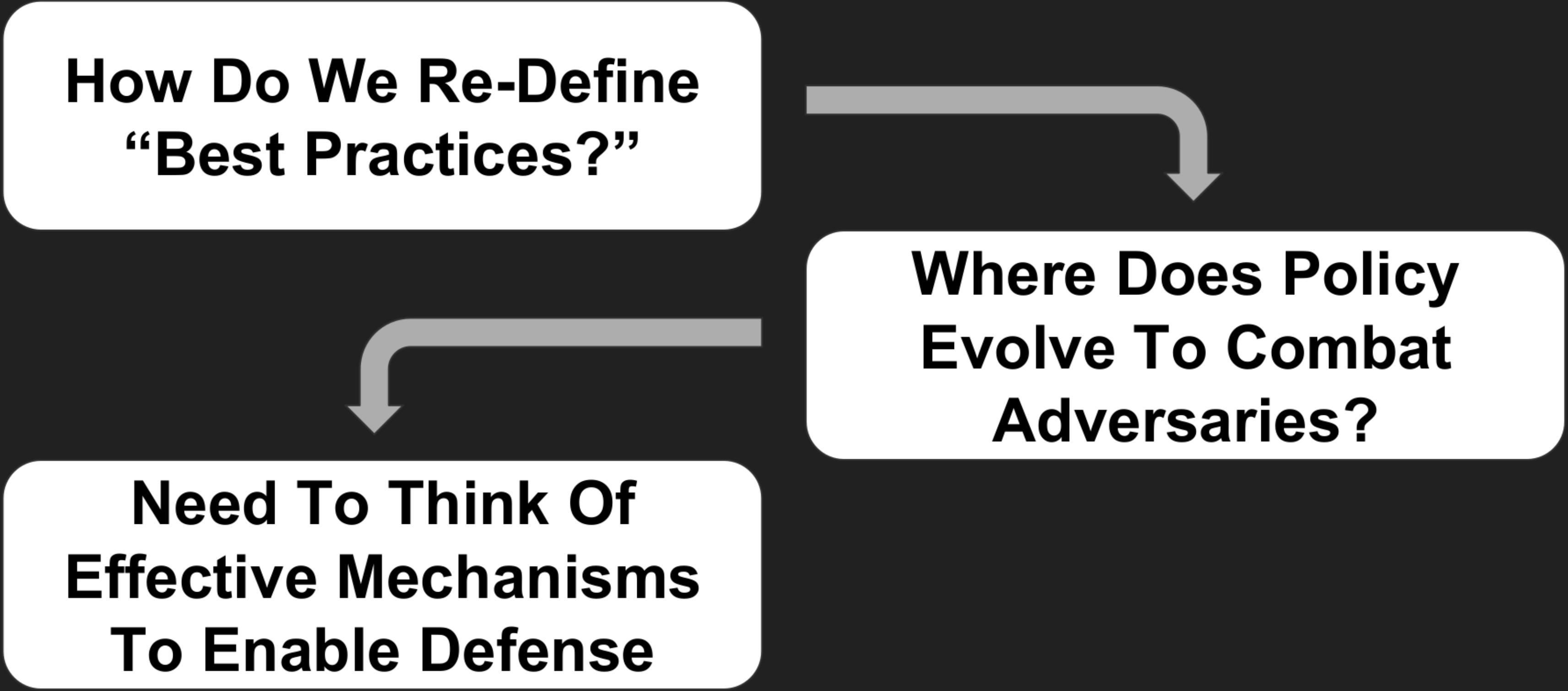
Policy Concerns



How Do We Re-Define “Best Practices?”

Where Does Policy Evolve To Combat Adversaries?

Policy Concerns



How Do We Re-Define “Best Practices?”

Where Does Policy Evolve To Combat Adversaries?

Need To Think Of Effective Mechanisms To Enable Defense

Conclusions

Complex Adversaries

Defenders & System Owners Must Understand Adversaries As Complex But Efficient Entities, With Implications For Operations & Mechanisms.

Complex Adversaries

Defenders & System Owners Must Understand Adversaries As Complex But Efficient Entities, With Implications For Operations & Mechanisms.

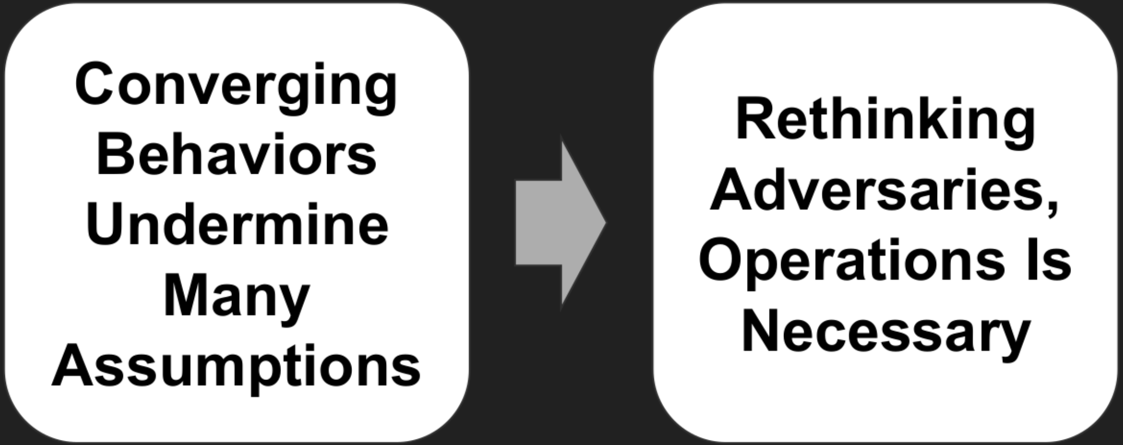
Multiple Implications In Terms Of Adversary Relationships, Converging Behaviors, & Impacts On How Operations “Look” To Defenders

Converging Behaviors

Converging Behaviors

Converging Behaviors Undermine Many Assumptions

Converging Behaviors



Converging Behaviors Undermine Many Assumptions

Rethinking Adversaries, Operations Is Necessary

Converging Behaviors

Converging Behaviors Undermine Many Assumptions

Rethinking Adversaries, Operations Is Necessary

Identify Opportunities Where They Exist!

Defender Opportunities

Defender Opportunities

Converged Tradecraft Means Defenders Have A More Focused Set To Target For Detection!

Defender Opportunities

Converged Tradecraft Means Defenders Have A More Focused Set To Target For Detection!

Preferred Behaviors Are HARD To Identify Though - Need To Improve Our Own Capabilities!

Defender Opportunities

Converged Tradecraft Means Defenders Have A More Focused Set To Target For Detection!

Preferred Behaviors Are HARD To Identify Though - Need To Improve Our Own Capabilities!

Migration To Behavior-Based Detection & Response Can Enable Significant “Wins”

Final Thoughts

Understanding Things - Adversaries, Intrusions, Etc. - As They ARE Requires Understanding Inherent Complexity.

YET Such Understanding Also Yields Opportunities For Response!

Questions?

Contact Info:

- *joe@paralus.co*
- *@jfslowik*
- *Signal (Talk To Me First!)*