Intelligence-Driven Response

for combating the Advanced Persistent Threat

July 2010

Michael Cloppert
Intel Fusion lead
Lockheed Martin CIRT

At Issue

Threat has shifted

Distinct strategic objective: CNE

Existing tools focus on vulnerability

Existing processes assume compromise

Alternate method of CND: Security Intelligence

Up Front

Examples used are concocted, OSINT derived

- Easy illustration of model
- Follow typical attack patterns of APT
- Key is application of techniques, finding useful indicator types

SecIntel leverages persistence against adversary

- Not effective against opportunistic threats (may be globally?)
- Expensive
- Must be applied with care

Better model, likely not best.

The Myth of Sophistication

Myth	Reality
What adversary "would do"	Minimal effort
Rejection of techniques as "amateur"	Maximize efficiency
Supported by assumption	Escalate as necessary
	Supported by observation

Assumptions risk underestimation of adversary

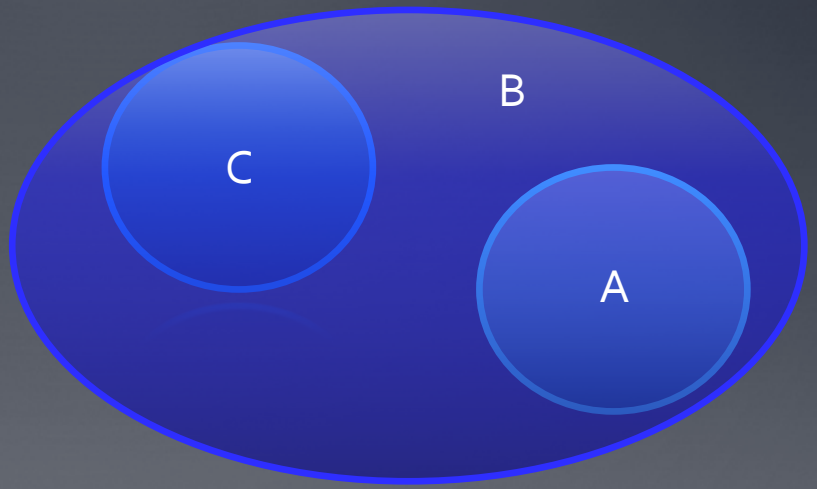
CND as Threat Mitigation

Indicators

Atomic

Computed

Behavioral



Mutability = Volatility^{-1}

What makes an immutable indicator?

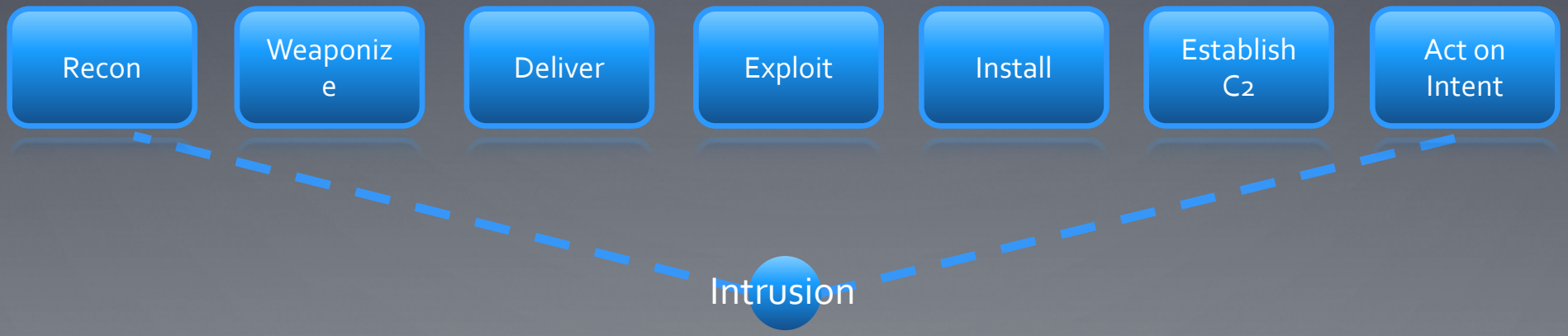
Where do indicators come from?

Model the Adversary's Tradecraft

To mitigate threat, must define it

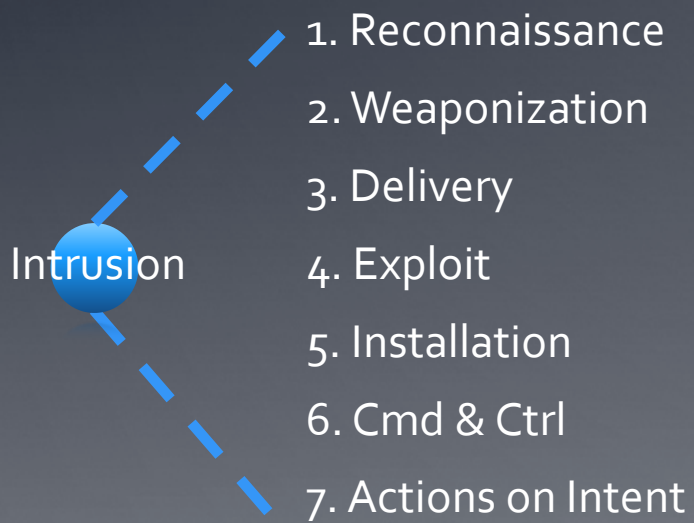
7-stage progression, aka "Kill Chain"

Framework for response



The Modern APT Kill Chain

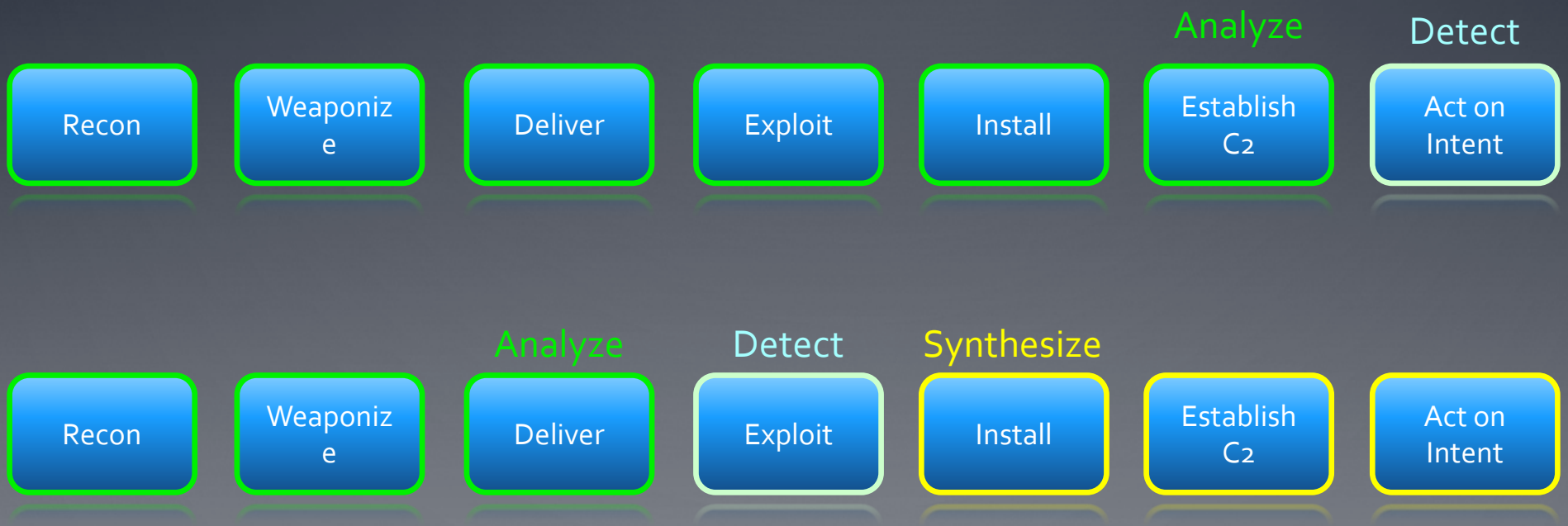
Terms don't mean what they once did



Old & Busted	New Hotness
Scanning, opportunistic	OSINT, targeted
Layer 4 payload	Layer 7 payload
Vuln protocol	Standard Comm. Prot.
Server-side (svc)	Client-side (app)
Plain sight	ADS, anti-reversing
Custom protocol	Protocol compliant
Propogate or PII	Exfiltrate

Kill Chain :: Complete Analysis

End-to-end understanding is goal



Indicator Courses of Action

Indicators are actionable intelligence

Action considers impact on intel

Completeness = resiliency

Gaps identify requirements

	Detect	Deny	Disrupt	Degrade	Deceive
1. Reconnaissance					Baited website
2. Weaponization	Metadata				
3. Delivery		Relay IP			Intercept
4. Exploit	.js emulator				
5. Installation				Non-admin	
6. Cmd & Ctrl			Content replace		
7. Actions on Intent	HIPS rules				

Completeness is temporally 2D

Actions looking forward are many

Singular action looking backward

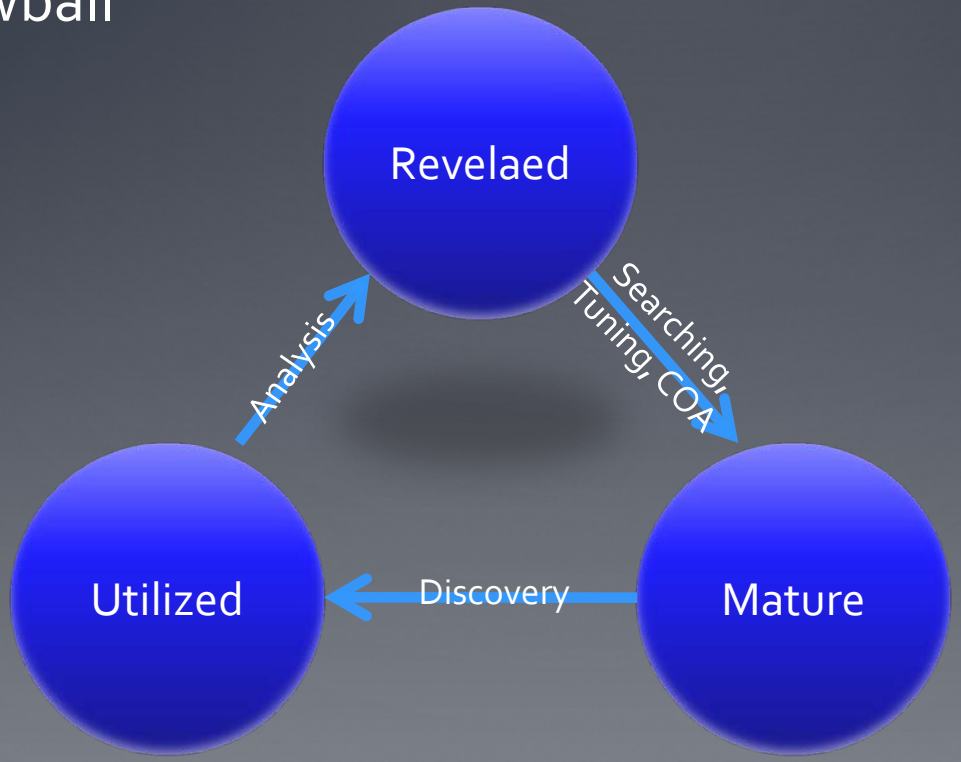
Inability to look backward leads to incomplete analysis

Searching drives additional requirements

The Indicator Lifecycle

Actionable intel has a lifecycle

"Intel Snowball"

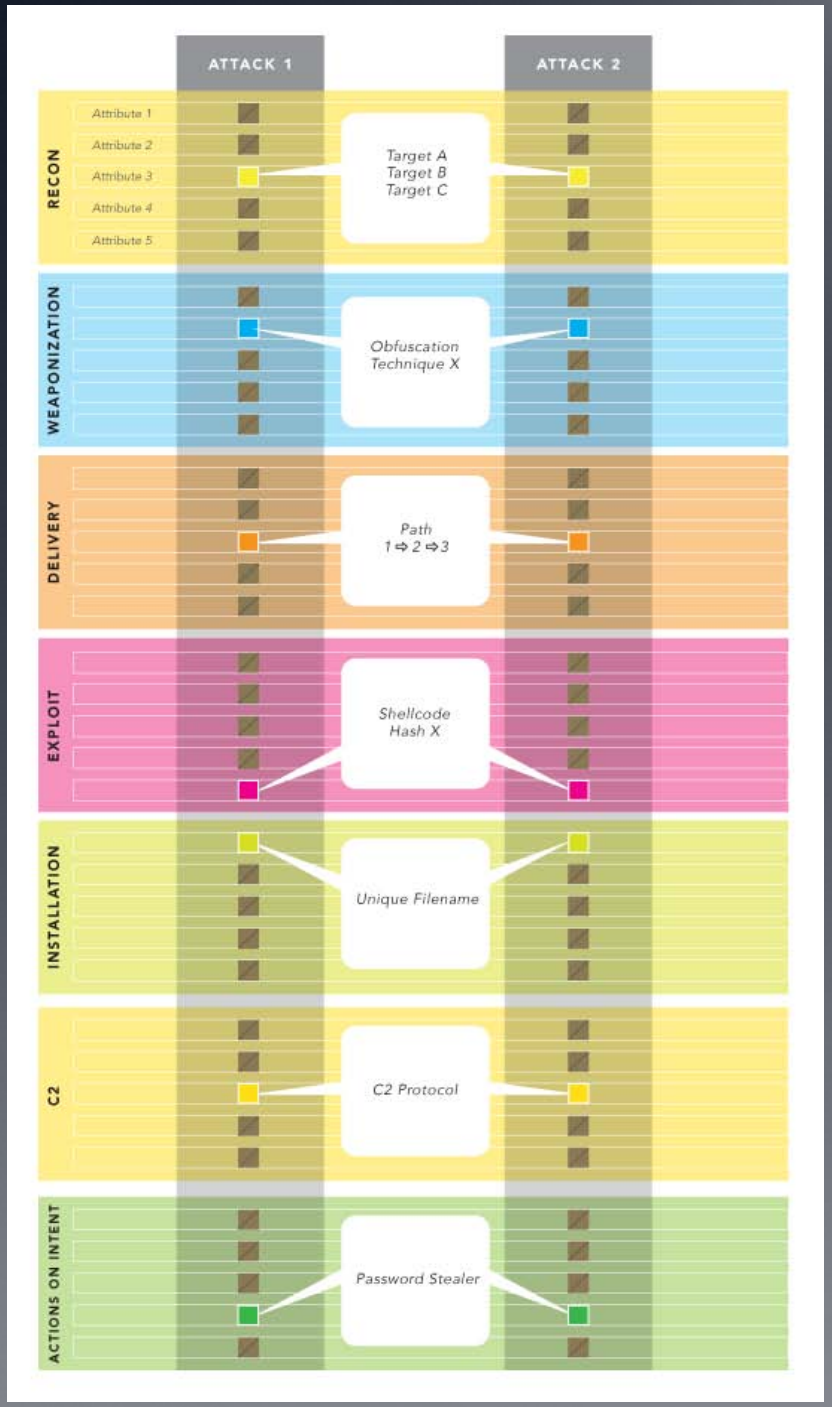


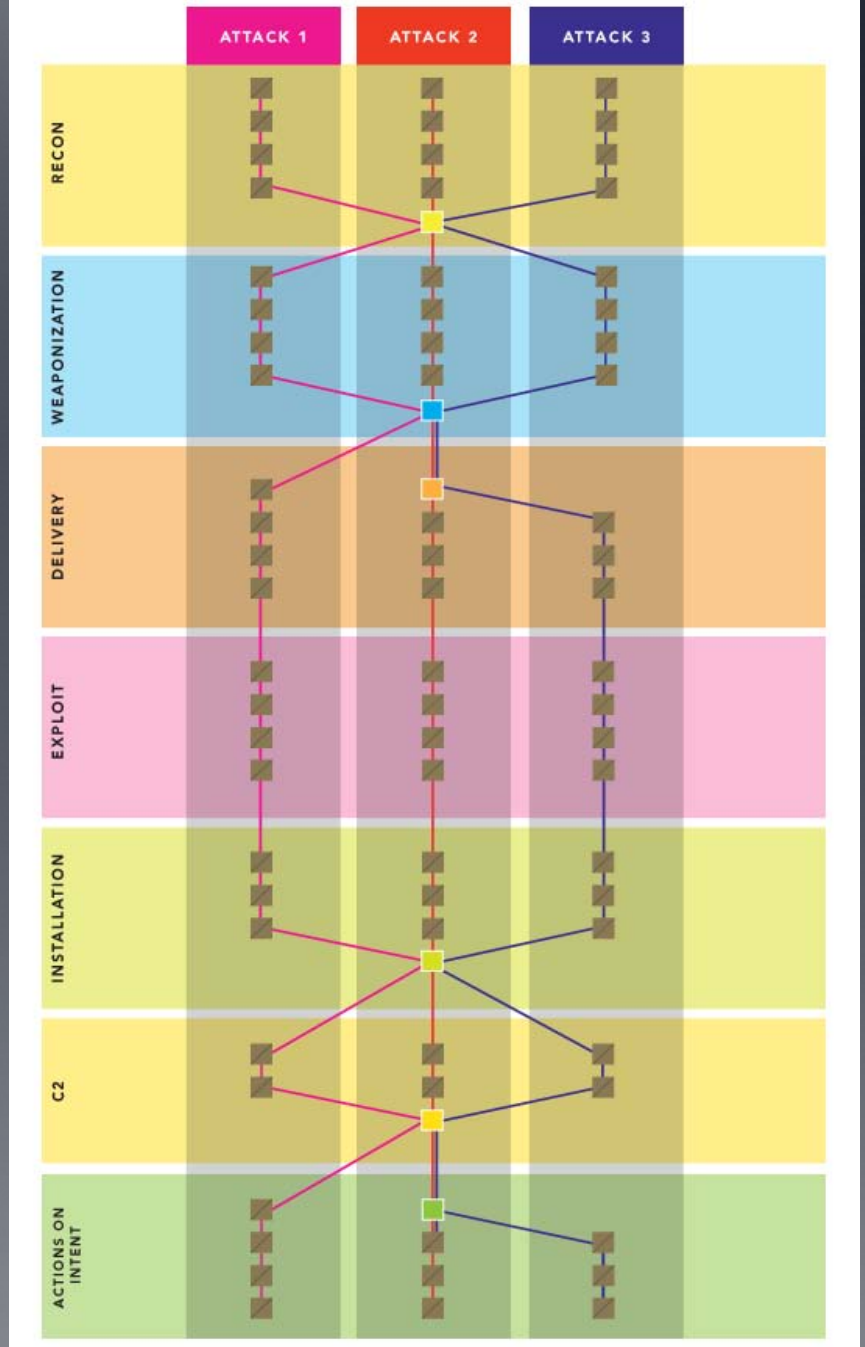
Patternicity

Analysis shows repeatable patterns

Projection of persistence

Linking on patterns forms campaigns


ATTACK 1
ATTACK 2
RECON
Attribute 1
Attribute 2
Attribute 3
Attribute 4
Attribute 5
Target A
Target B
Target C
WEAPONIZATION
Obfuscation Technique X
DELIVERY
Path 1 ⇨ 2 ⇨ 3
EXPLOIT
Shellcode Hash X
INSTALLATION
Unique Filename
C2
C2 Protocol
ACTIONS ON INTENT
Password Stealer


ATTACK 1
ATTACK 2
ATTACK 3
RECON
WEAPONIZATION
DELIVERY
EXPLOIT
INSTALLATION
C2
ACTIONS ON INTENT

	Attack 1	Attack 2	Attack 3
Recon	10.23.156.130		
Weap	"Python PDF Library" unknown.pdf	**"Python PDF Library"** **unknown.pdf**	
Delivery	jane.doe@gmail.com A07-20536AF-35Broc.pdf(?) (.sig)(?)	**jane.doe@gmail.com** **(.sig)(?)**	
Exploit	(shellcode)	(shellcode')	
Install	%LST%\svchost.exe HKCU\…\Run\svchost (svchost MD5)	**%LST%\svchost.exe** **HKCU\…\Run\svchost** (svchost MD5')	…
C2	/cutenews/…/gFr554.php www.newmoon-movie.net (signature)	**/cutenews/…/gFr554.php** **10.23.156**.180 **(signature)**	/1314563/fgDc43.php **10.23.156.180** (signature')
Actions	ntfre.exe Pwdumpx.exe dumpext.dll dumpsvc.exe		

Results

Defender:

- Detection pushed up kill chain to pre-compromise
- "Only have to be right once"
- Threat-driven investment
- 0-day risk mitigated
- Collaboration amplifies benefits

Aggressor:

- Cost of success increases
- Likelihood decreases
- Persistence catch-22

Impacts of Intel Gaps

Indicator lifecycle broken

Intel becomes stale

Attrition / drift reduces completeness of campaigns

New techniques / opportunities unidentified

…

Intrusions go undetected

Adversaries complete objectives

All your base…

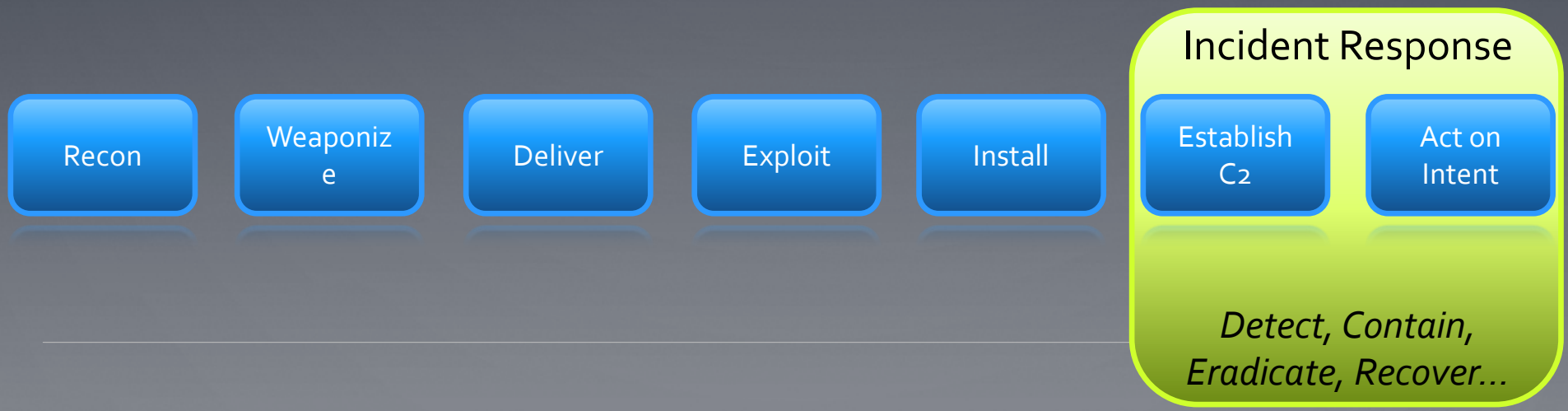
Comparison to Classic IR Process

2008: "Classic IR process is insufficient against APT"

Response focuses on post-compromise

Focus on vulnerability, not threat

Incompatible linear process, views attacks in isolation



Getting There…

Focus on techniques, requirements

Select tools

Prioritize research

Identify platforms, not turnkey solutions

- Network
- Host

Define processes

Hire analysts, dev/analysts, developers

man SecIntel

```
SecIntel(1)          CND General Techniques Manual          SecIntel(1)

NAME
    SecIntel – Security Intelligence; Methods for combating the APT

AUTHOR
    Michael Cloppert

CREDITS
    LM-CIRT team members

SEE ALSO
    email(mike@cloppert.org)
    twitter(mikecloppert)
    web(http://blog.cloppert.org/)
    web(https://blogs.sans.org/computer-forensics/author/mikecloppert/)


CND                          July 2010                          CND
(END)
```