FireEye

Enterprise Security Monitoring

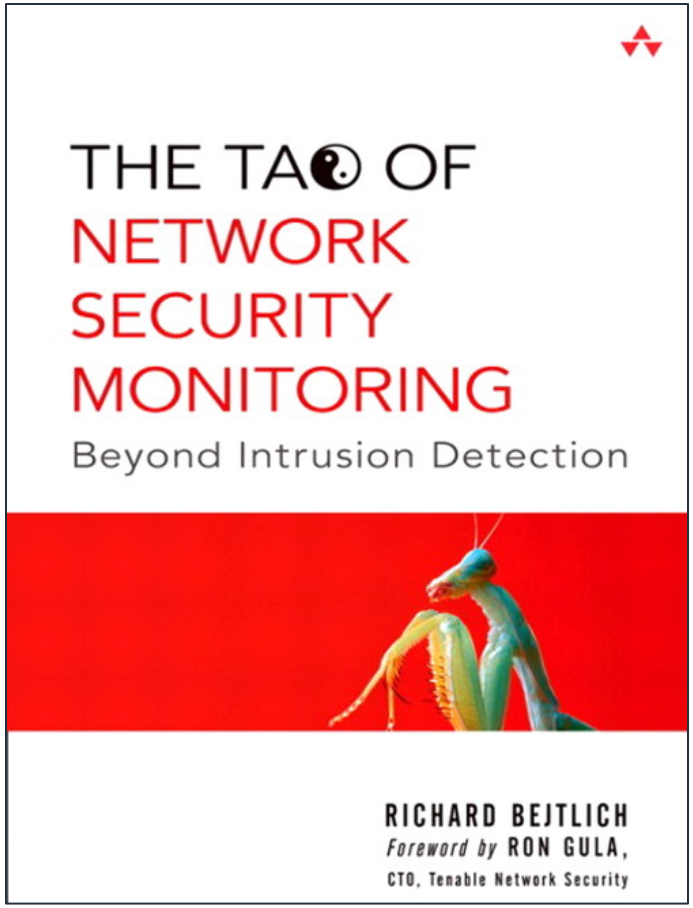
Comprehensive Intel-Driven Detection

David J. Bianco
David.Bianco@mandiant.com

First There Was…

FireEye

Then There Was…



FireEye

Now There Is…

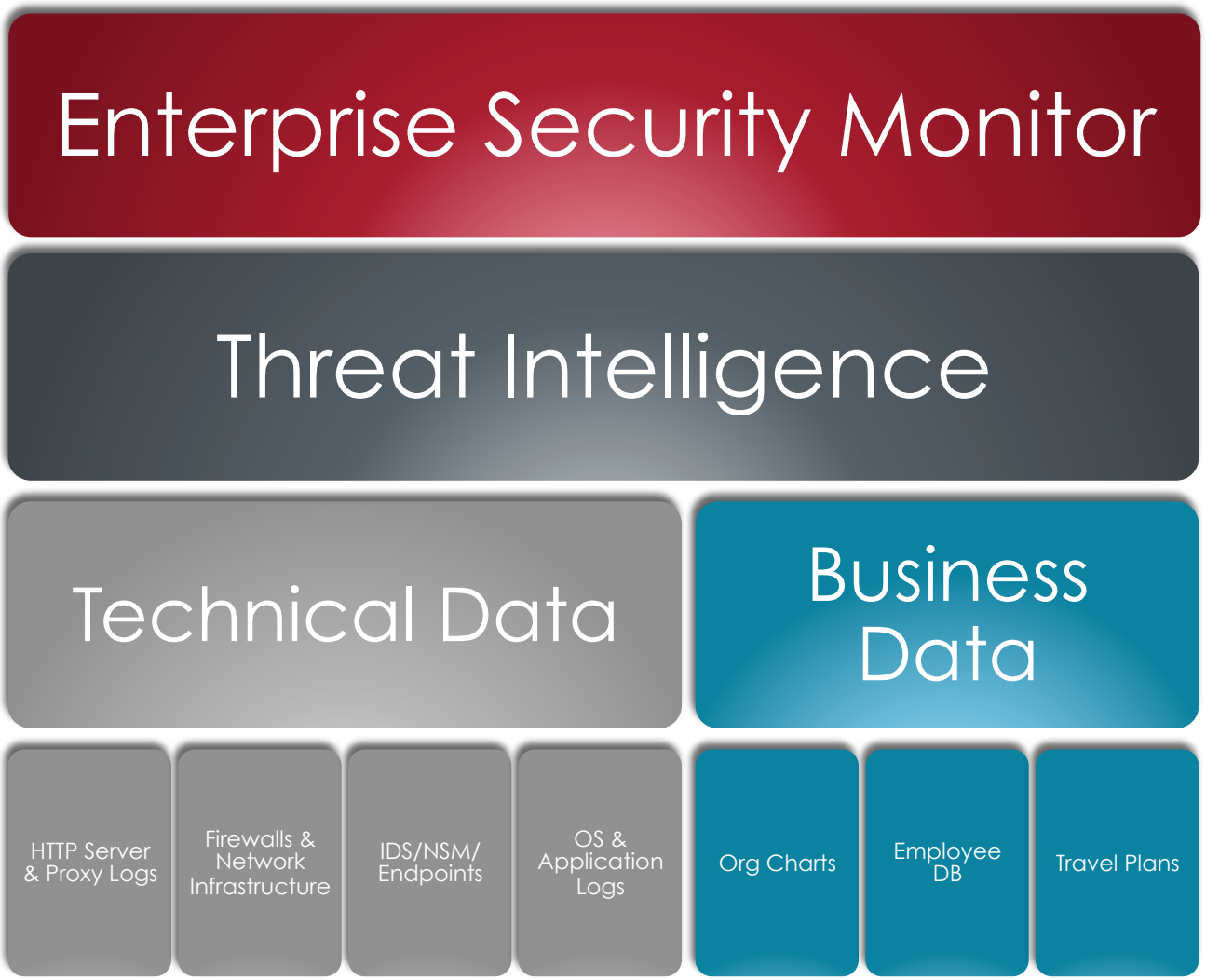
Enterprise Security Monitoring (ESM)

FireEye

Enterprise Security Monitoring

FireEye

ESM Architecture



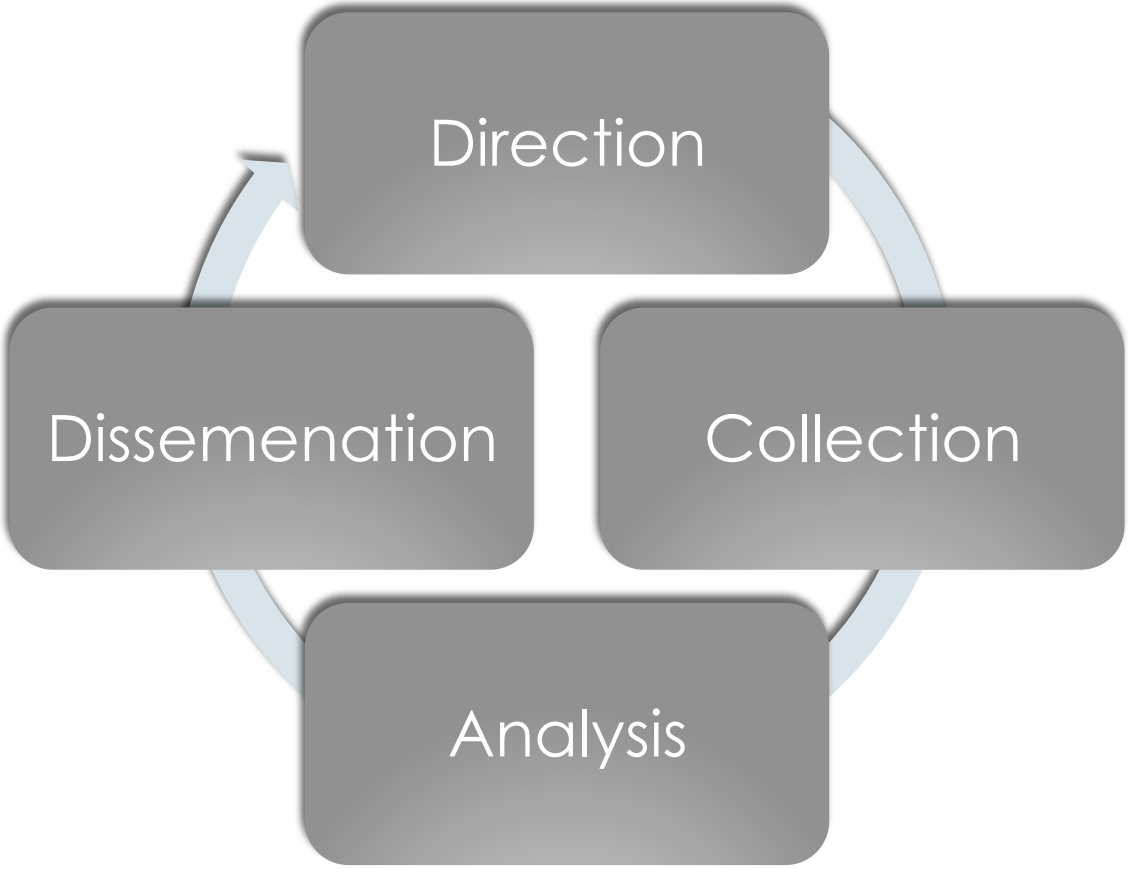
FireEye

Benefits of Enterprise Security Monitoring

- Increased visibility across the organization
- Get more value out of existing systems
- Data aggregation is hunter friendly
- Better organization around:
  - Detection platform coverage
  - Detection planning
    - General
    - Threat-specific
  - Prioritization of detection resources
- Quicker, more accurate incident detection and response
- Leverage your detection/response infra as an offensive capability

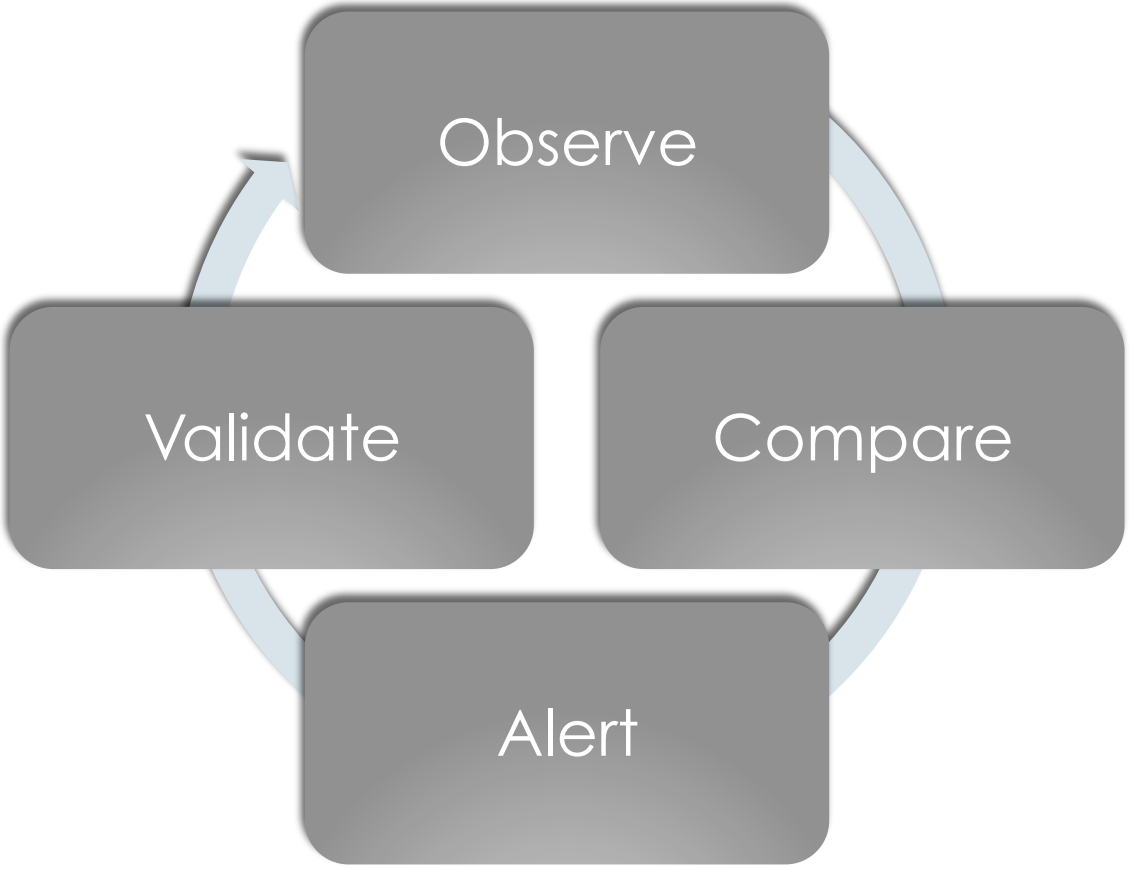
FireEye

Intel Lifecycle



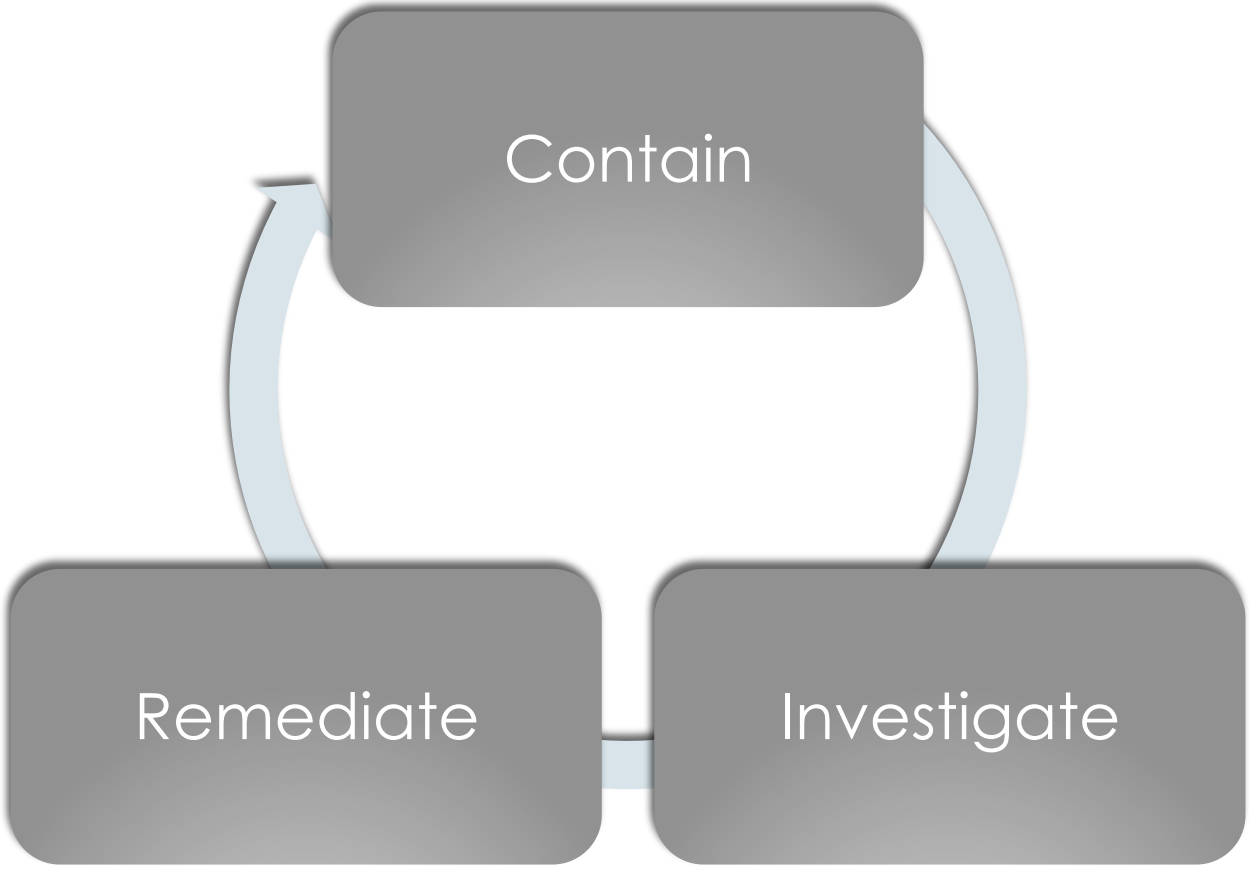
FireEye

Detection Process



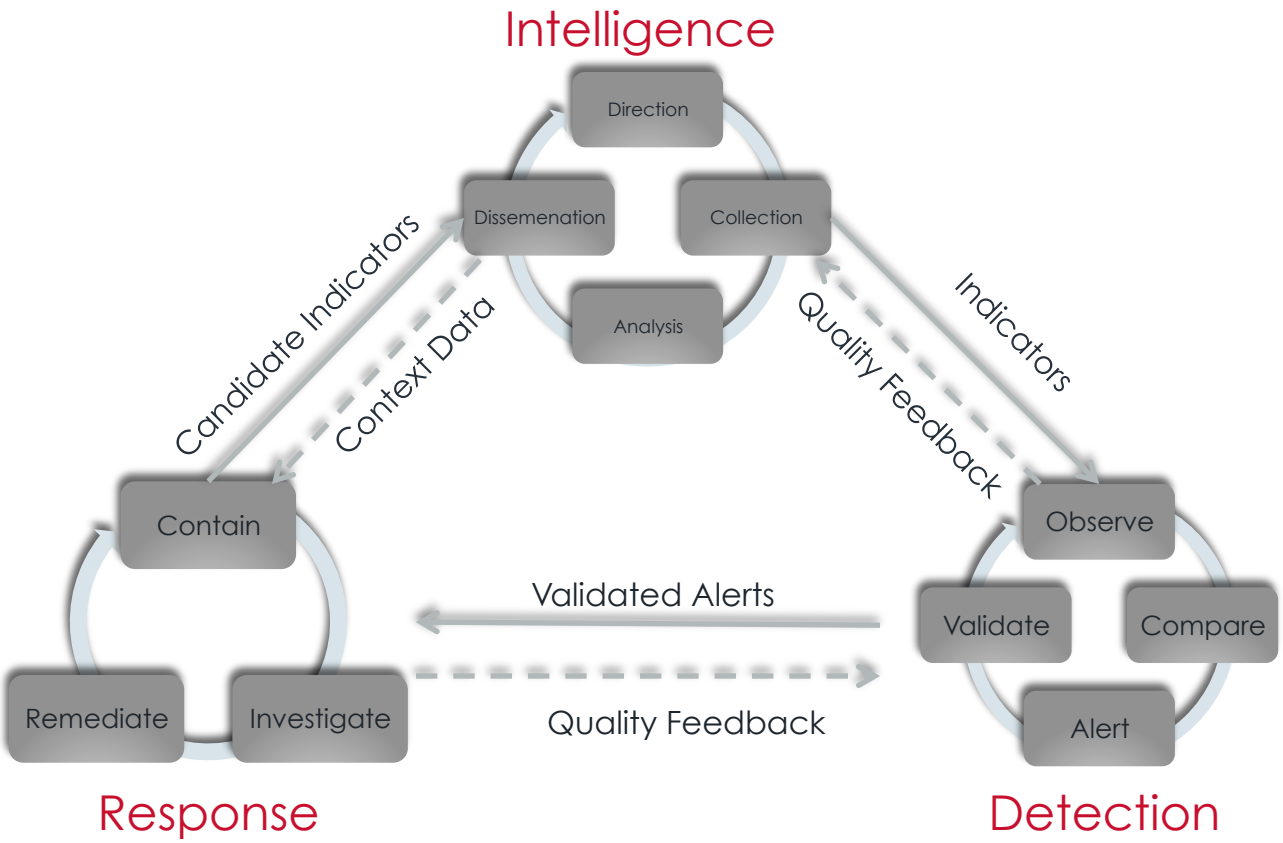
FireEye

Response Cycle



FireEye

The Intel-Driven Operations Cycle



FireEye

Wacky Wall Walker Intelligence

The most common approach to "threat intel" I see is…

THROW ALL OUR FACTS OUT THERE AND SEE WHAT STICKS.

Pros	Cons
Quick to implement	Too many alerts No confidence in results Gives your adversaries a laugh

We can do better!

FireEye

Let's Be Clear…

Most people confuse  with intelligence.

Let's Be Clear…

Captain, I do not believe that to be the correct use of the term.

What is an Indicator?

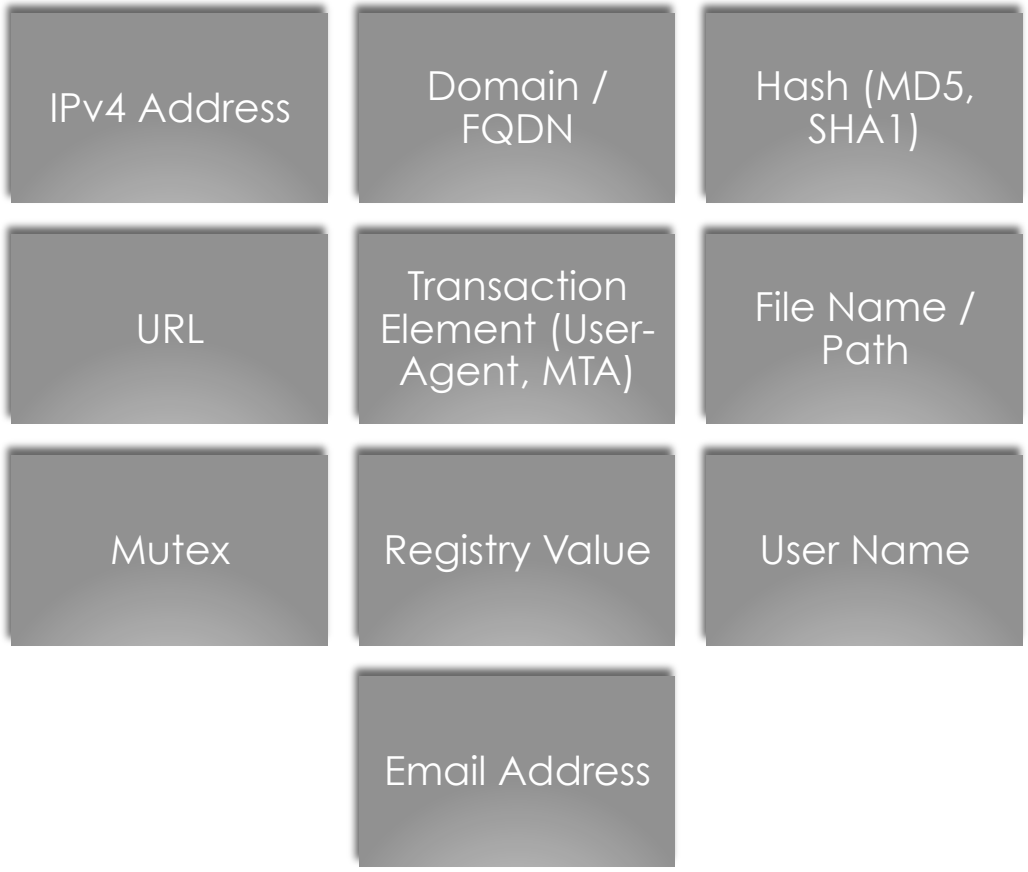
A piece of information that points to a certain conclusion

What is it Not?

≠

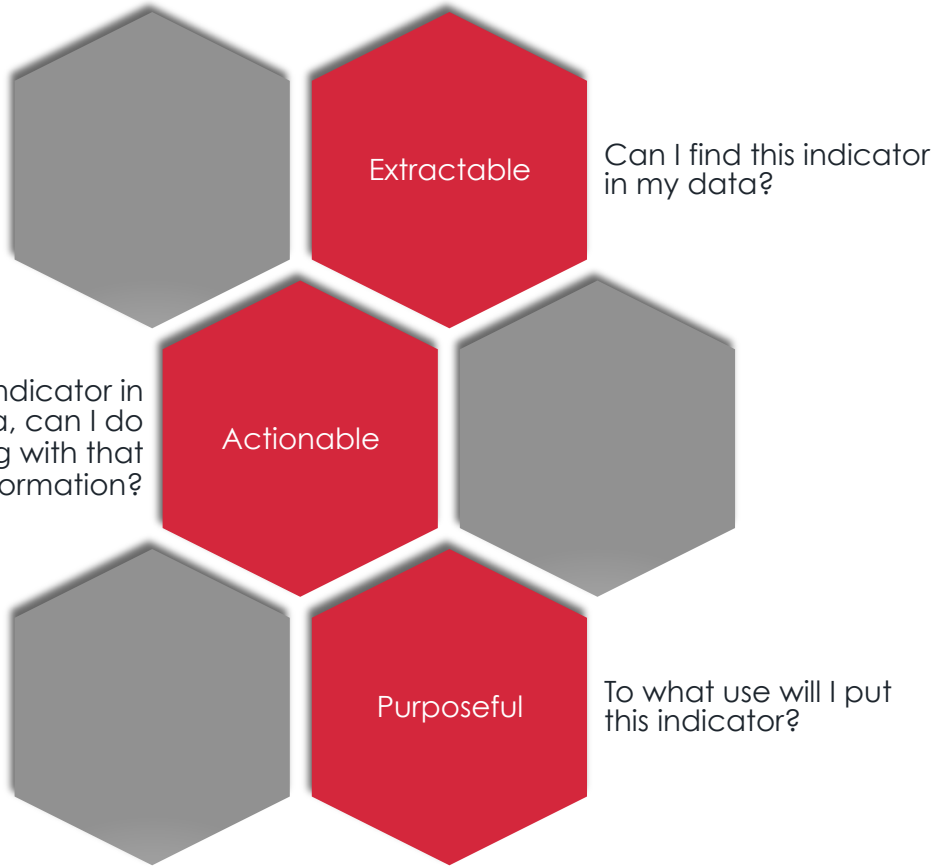
FireEye

Common Indicator Data Types



FireEye

Indicator Characteristics



FireEye

Indicator Purposes

Attribution

- Who/what is responsible for this activity?

Detection

- If this event happens, I want to know about it.

Profiling

- What are the targeting parameters for this threat?

Prediction

- Given the current state, what can I expect from this threat in the future?

FireEye

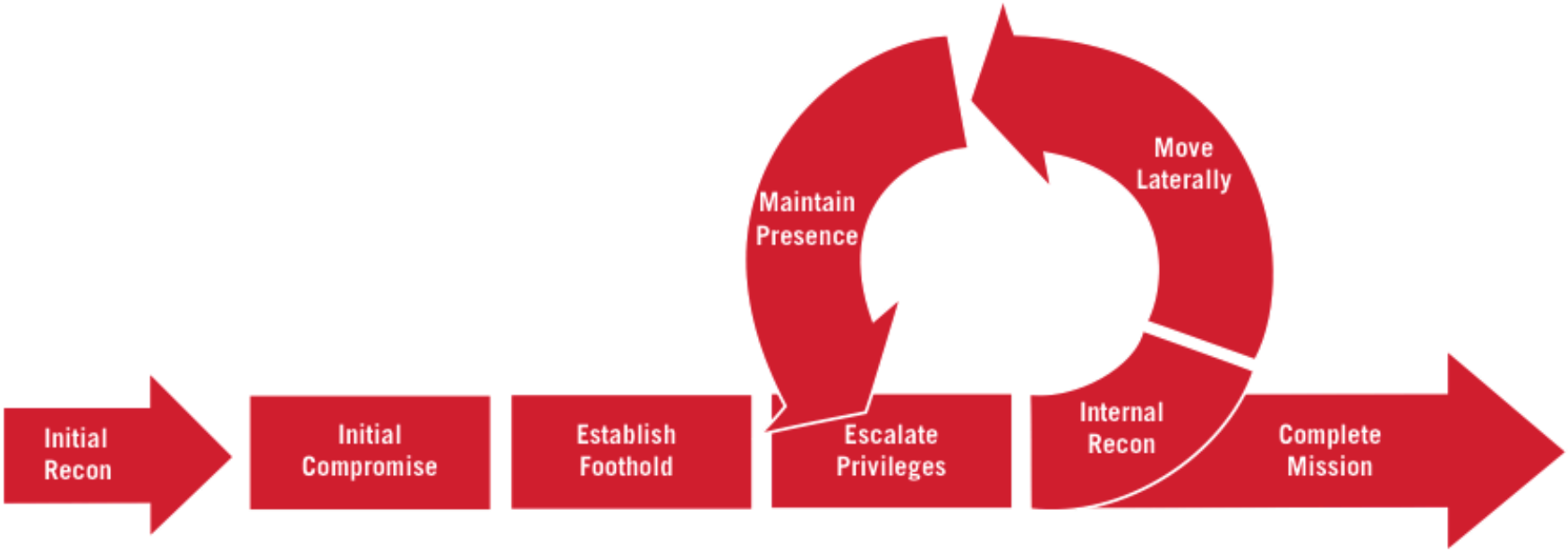
The Kill Chain

"[…] a systematic process to target and engage an adversary to create desired effects."

Source: *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains"*, Hutchins, Cloppert, Amin, http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf (Last checked August 2013)

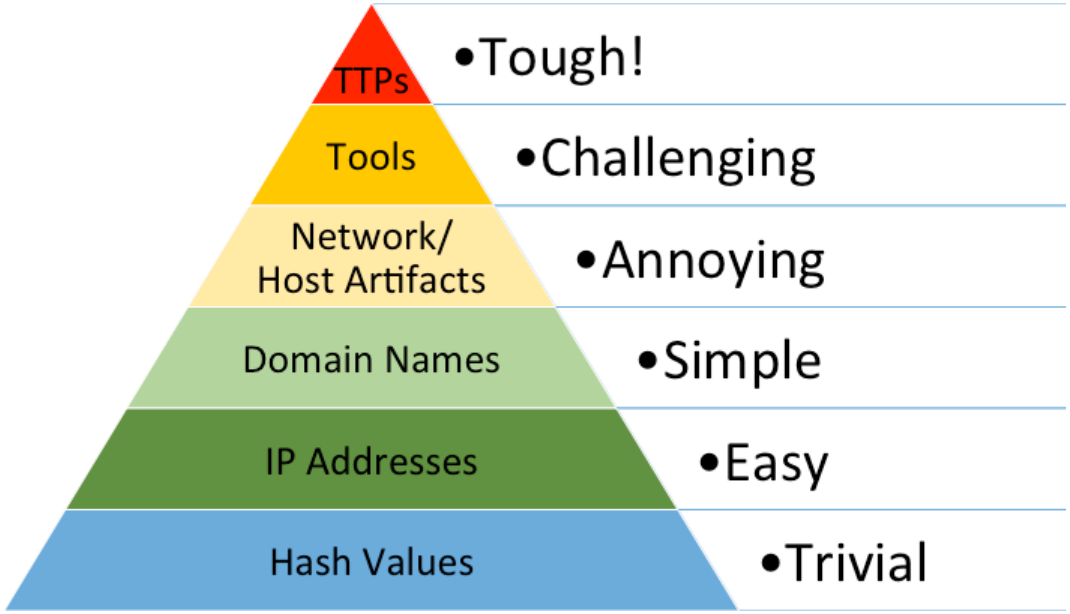
FireEye

Mandiant Attack Lifecycle Diagram



FireEye

The Pyramid of Pain



The Pyramid measures potential usefulness of your intel

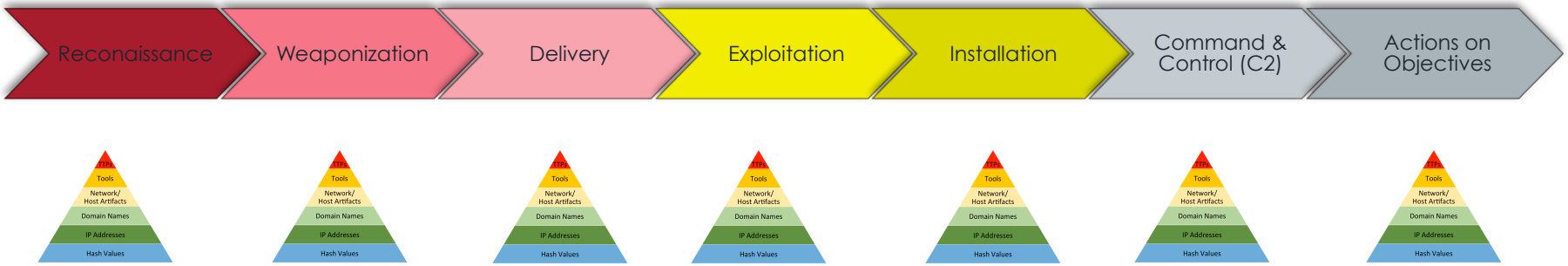
It also measures difficulty of obtaining that intel

The higher you are, the more resources your adversaries have to expend.

When you quickly detect, respond to and disrupt your adversaries' activities, defense becomes offense.

FireEye

The Bed of Nails

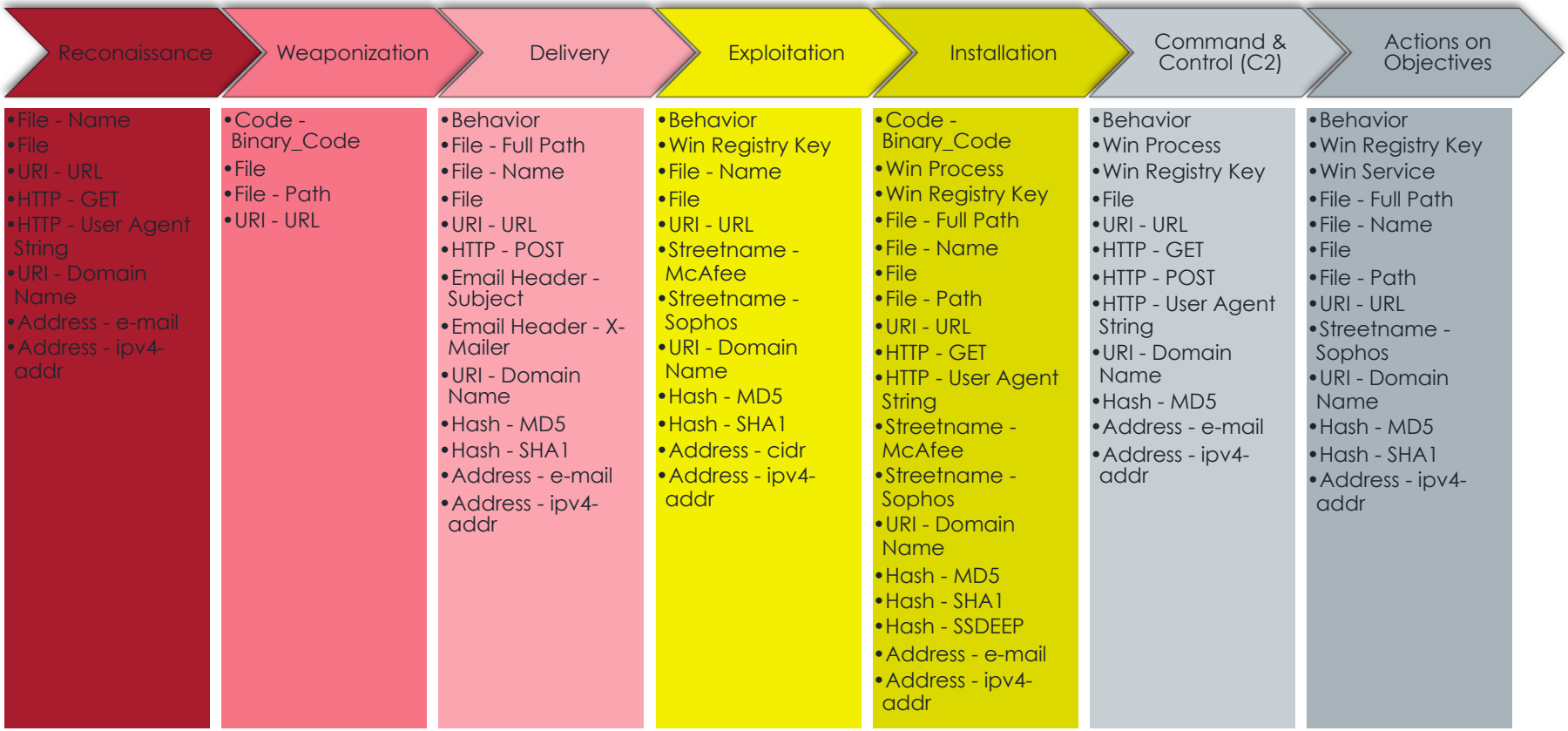


Intel-Driven Detection Planning

- What scenarios do we need to be able to detect?
- What are our options for detecting them?
- What are the strengths and weaknesses of our detection program today?
- What is our detection stance against specific actors?
- What is our overall plan for detection across our enterprise?

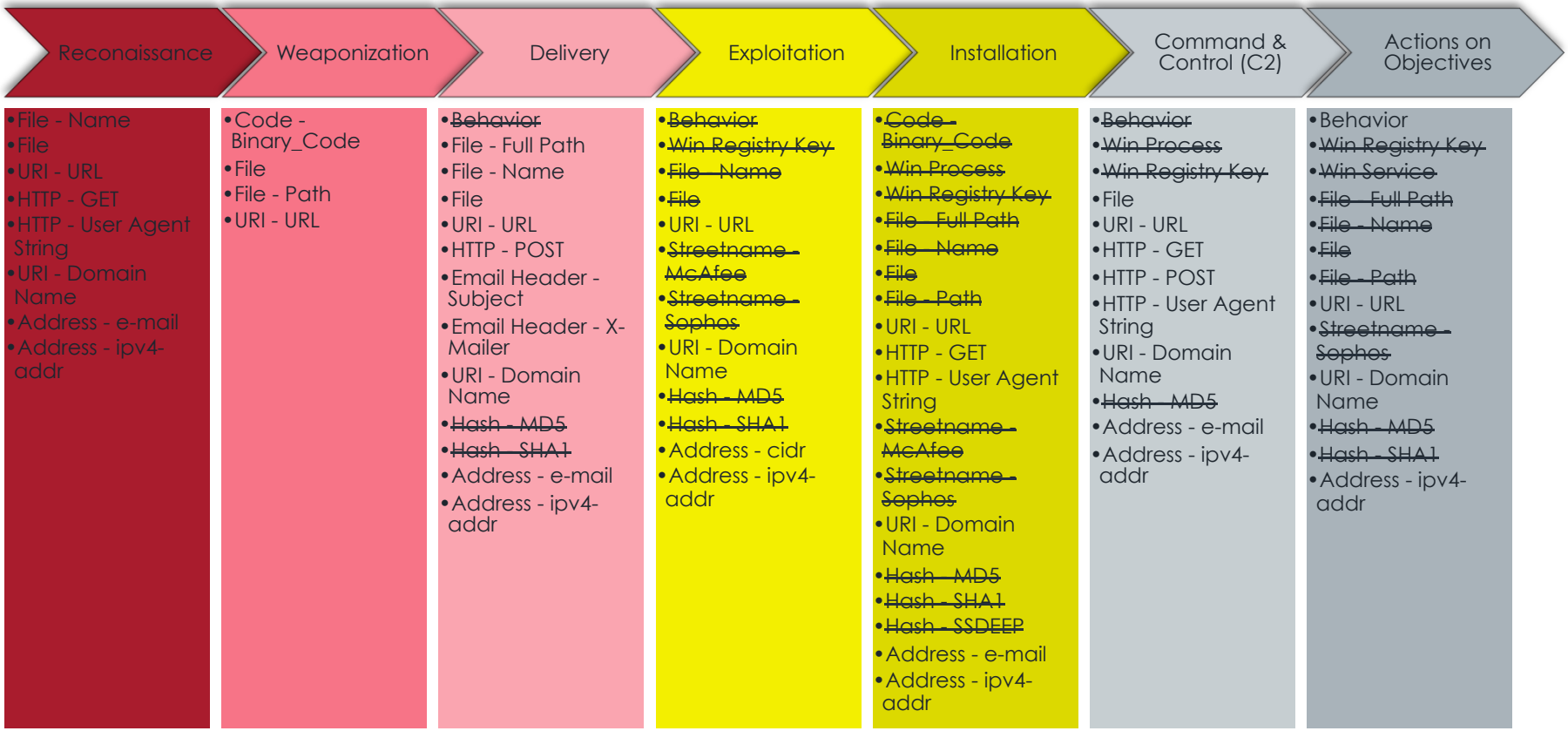
FireEye

What Scenarios Do We Need to Detect?

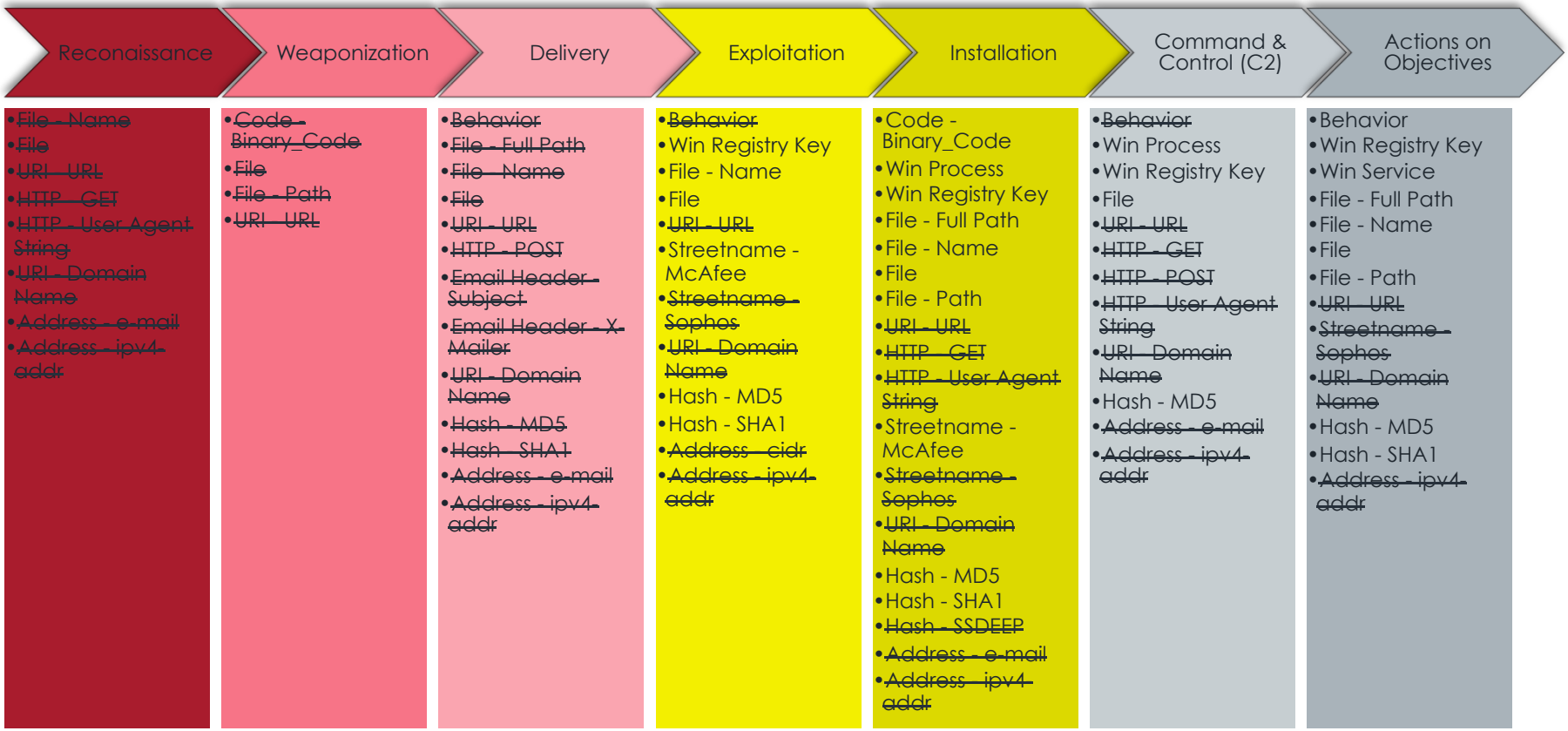


FireEye

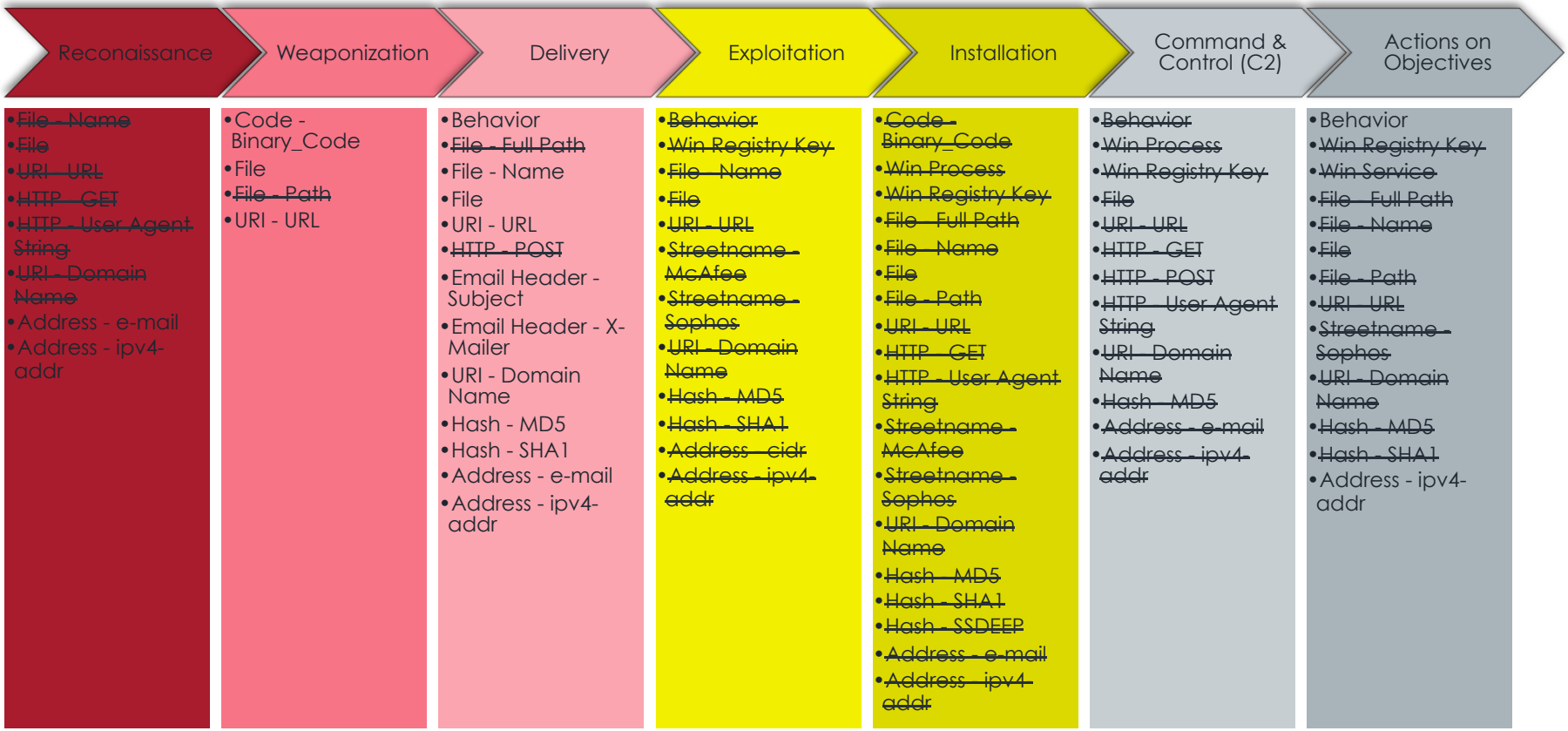
Detection Options - Snort



Detection Options - HIPS



Detection Options – Email Gateway Logs



Score Card: Use of Available Indicators

Reconaissance	Weaponization	Delivery	Exploitation	Installation	Command & Control (C2)	Actions on Objectives
• File - Name • File • URI - URL • HTTP - GET • HTTP - User Agent String • URI - Domain Name • Address - e-mail • Address - ipv4-addr	• Code - Binary_Code • File • File - Path • URI - URL	• Behavior • File - Full Path • File - Name • File • URI - URL • HTTP - POST • Email Header - Subject • Email Header - X-Mailer • URI - Domain Name • Hash - MD5 • Hash - SHA1 • Address - e-mail • Address - ipv4-addr	• ~~Behavior~~ • Win Registry Key • File - Name • File • URI - URL • Streetname - McAfee • ~~Streetname - Sophos~~ • URI - Domain Name • Hash - MD5 • Hash - SHA1 • Address - cidr • Address - ipv4-addr	• Code - Binary_Code • Win Process • Win Registry Key • File - Full Path • File - Name • File • File - Path • URI - URL • HTTP - GET • HTTP - User Agent String • Streetname - McAfee • ~~Streetname - Sophos~~ • URI - Domain Name • Hash - MD5 • Hash - SHA1 • ~~Hash - SSDEEP~~ • Address - e-mail • Address - ipv4-addr	• ~~Behavior~~ • Win Process • Win Registry Key • File • URI - URL • HTTP - GET • HTTP - POST • HTTP - User Agent String • URI - Domain Name • Hash - MD5 • Address - e-mail • Address - ipv4-addr	• Behavior • Win Registry Key • Win Service • File - Full Path • File - Name • File • File - Path • URI - URL • ~~Streetname - Sophos~~ • URI - Domain Name • Hash - MD5 • Hash - SHA1 • Address - ipv4-addr

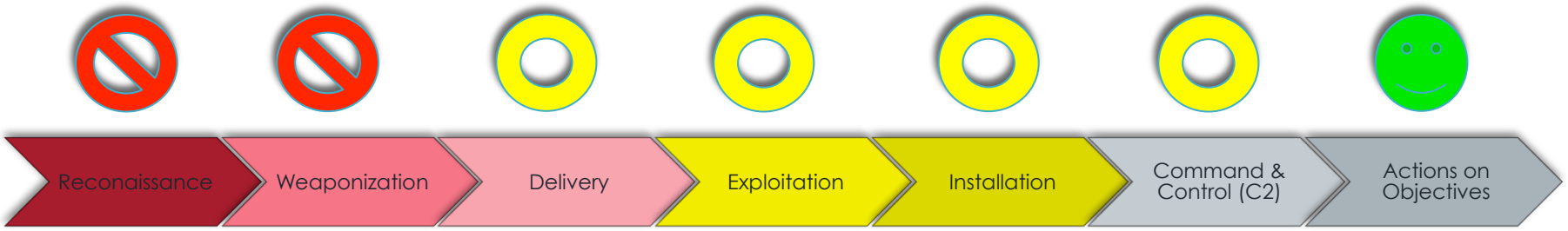
FireEye

Score Card: Pyramid Effectiveness of Indicators

Reconaissance	Weaponization	Delivery	Exploitation	Installation	Command & Control (C2)	Actions on Objectives
• File - Name • File • URI - URL • HTTP - GET • HTTP - User Agent String • URI - Domain Name • Address - e-mail • Address - ipv4-addr	• Code - Binary Code • File • File - Path • URI - URL	• Behavior • File - Full Path • File - Name • File • URI - URL • HTTP - POST • Email Header - Subject • Email Header - X-Mailer • URI - Domain Name • Hash - MD5 • Hash - SHA1 • Address - e-mail • Address - ipv4-addr	• Behavior • Win Registry Key • File - Name • File • URI - URL • Streetname - McAfee • Streetname - Sophos • URI - Domain Name • Hash - MD5 • Hash - SHA1 • Address - cidr • Address - ipv4-addr	• Code - Binary_Code • Win Process • Win Registry Key • File - Full Path • File - Name • File • File - Path • URI - URL • HTTP - GET • HTTP - User Agent String • Streetname - McAfee • Streetname - Sophos • URI - Domain Name • Hash - MD5 • Hash - SHA1 • Hash - SSDEEP • Address - e-mail • Address - ipv4-addr	• Behavior • Win Process • Win Registry Key • File • URI - URL • HTTP - GET • HTTP - POST • HTTP - User Agent String • URI - Domain Name • Hash - MD5 • Address - e-mail • Address - ipv4-addr	• Behavior • Win Registry Key • Win Service • File - Full Path • File - Name • File • File - Path • URI - URL • Streetname - Sophos • URI - Domain Name • Hash - MD5 • Hash - SHA1 • Address - ipv4-addr

FireEye

Score Card: Effectiveness Against APT-π



Reconaissance	Weaponization	Delivery	Exploitation	Installation	Command & Control (C2)	Actions on Objectives
• URI – Domain Name • Address - ipv4-addr		• Email Header - Subject • Email Header - X-Mailer • URI - Domain Name • ~~Hash - MD5~~ • ~~Hash - SHA1~~ • Address - e-mail • Address - ipv4-addr	• Win Registry Key • File - Name • File • URI - URL • Streetname - McAfee • URI - Domain Name • Hash - MD5 • Hash - SHA1 • Address - cidr • Address - ipv4-addr	• Code - Binary_Code • Win Process • Win Registry Key • File - Full Path • File - Name • File • File - Path • URI - URL • HTTP - GET • HTTP - User Agent String • Streetname - McAfee • URI - Domain Name • Hash - MD5 • Hash - SHA1 • Address - ipv4-addr	• ~~Behavior~~ • Win Process • Win Registry Key • File • URI - URL • HTTP - GET • HTTP - POST • HTTP - User Agent String • URI - Domain Name • Hash - MD5 • Address - e-mail • Address - ipv4-addr	• Behavior • Win Registry Key • Win Service • File - Full Path • File - Name • File • File - Path • URI - URL • ~~Streetname - Sophos~~ • URI - Domain Name • Hash - MD5 • Hash - SHA1 • Address - ipv4-addr

FireEye

Enterprise Detection Plan

	Reconnaissance	Weaponization	Delivery	Exploitation	Installation	C2	Actions on Intent
Behavior			Email GW	NONE		NONE	Snort HIPS
Code - Binary_Code		Email GW			HIPS MIR		
Win Process					HIPS MIR	HIPS MIR	
Win Registry Key				HIPS MIR	HIPS MIR	HIPS MIR	HIPS MIR
Win Service							
File - Full Path			Snort		HIPS MIR		HIPS MIR
File - Name	Snort		Snort Email GW	HIPS MIR	HIPS MIR		HIPS MIR
File	Snort	Snort Email GW	Snort Email GW	HIPS MIR	HIPS MIR	HIPS MIR	HIPS MIR
File - Path		Snort			HIPS MIR		HIPS MIR
URI - URL	Snort	Snort Email GW	Snort Email GW	Snort	Snort	Snort	Snort
HTTP - GET	Snort				Snort	Snort	
HTTP - POST			Snort			Snort	
HTTP - User Agent String	Snort				Snort	Snort	
Email Header - String							
Email Header - Subject			Snort Email GW				
Email Header - X-Mailer			Snort Email GW				
Email Header - Message-ID							
Streetname - McAfee				HIPS	HIPS		
Streetname - Sophos				NONE	NONE		NONE
URI - Domain Name	Snort		Snort Email GW	Snort	Snort		Snort
Hash - MD5			Email GW	HIPS MIR	HIPS MIR	HIPS MIR	HIPS MIR
Hash - SHA1			Email GW	HIPS MIR	HIPS MIR		HIPS MIR
Hash - SSDEEP					NONE		
Address - e-mail	Snort Email GW		Snort Email GW		Snort	Snort	
Address - cidr				Snort			
Address - ipv4-addr	Snort Email GW		Snort Email GW	Snort	Snort	Snort	Snort
Address - ipv6-addr							

FireEye

Summary

- NSM:IDS :: ESM:NSM
- Collect and aggregate across your entire enterprise
  - Increased visibility
  - Maximum use of resources
  - Better for hunting
- Organize intel for for better program insights
- Big improvements in detection & response capabilities for minimal investment
- Smart detection makes for frustrated adversaries!

FireEye

Questions?

David J. Bianco

David.Bianco@mandiant.com

@DavidJBianco

detect-respond.blogspot.com

I <3 Feedback!

I'd really love to hear from you. Questions, comments, stories about how this worked for you, citations referencing my work are all appreciated!

FireEye