



# Give yourself time in the fight against cyberattacks

With an integrated threat defense

Story Tweedie-Yates  
Head of Cisco Security Product Marketing in EMEAR  
December 2016

# Most interesting thing about Ukraine?

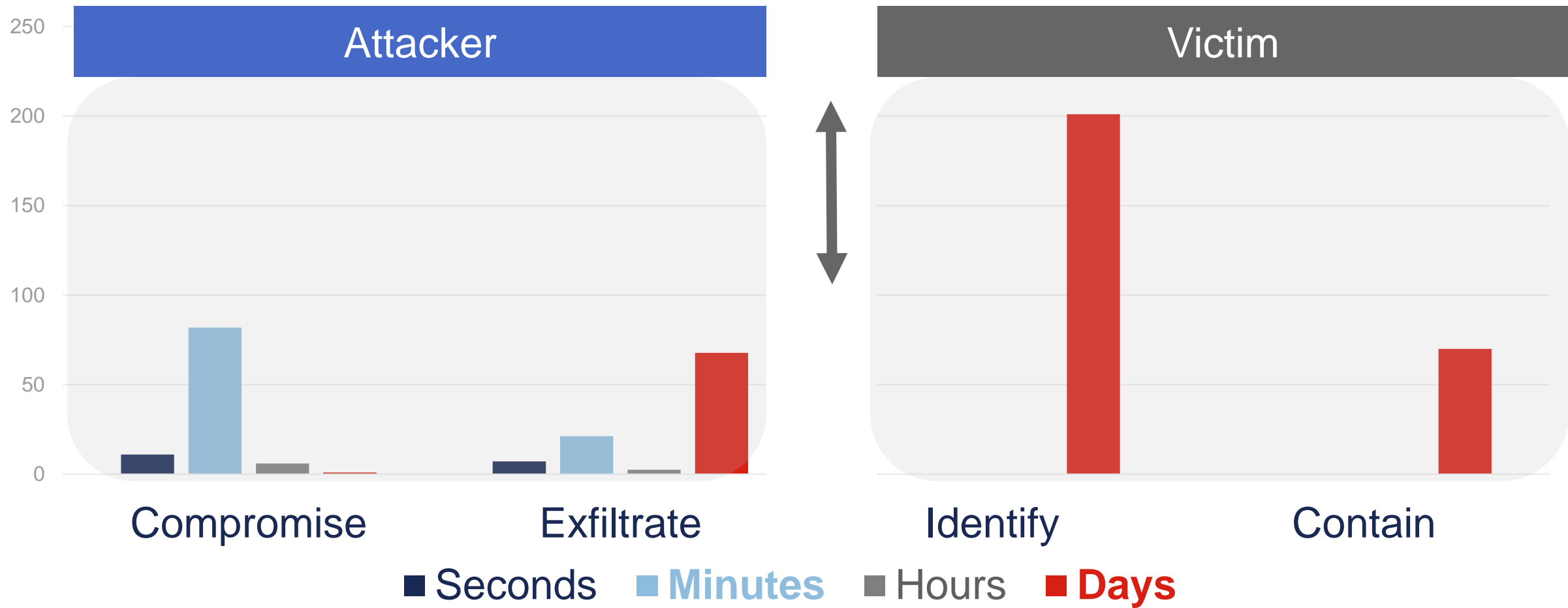
# Debunk “kill chain” misconception

## Your basic defense and attackers’ speed

## How Cisco lowers Total Time to Detection



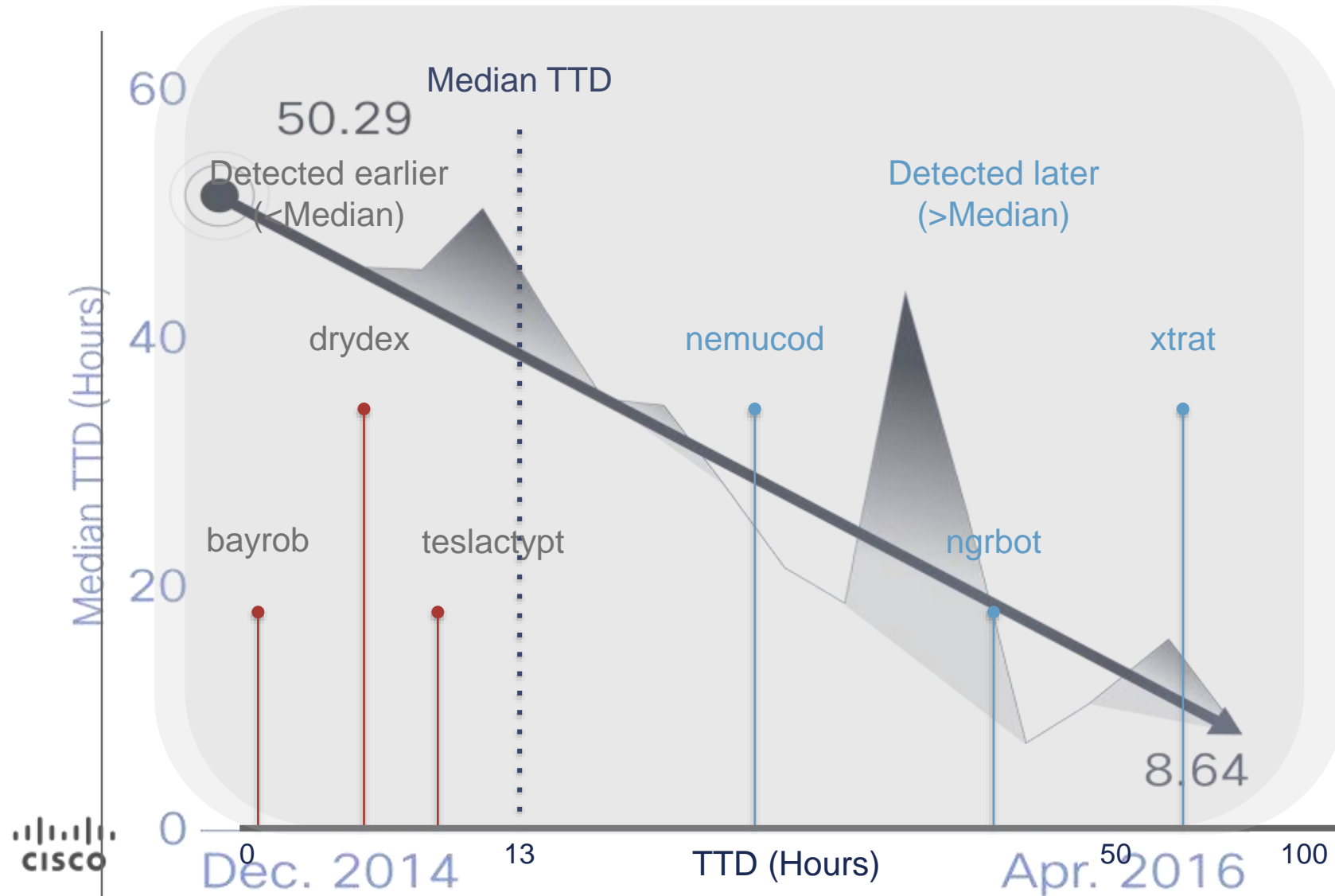
# Attackers are winning the battle for time





# Measure and improve your TTD

Gaining an edge on the continuous “arms race.”



# Is early protection the best way to lower TTD?





# Typical ransomware kill chain

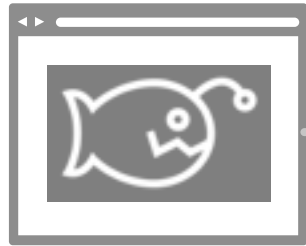
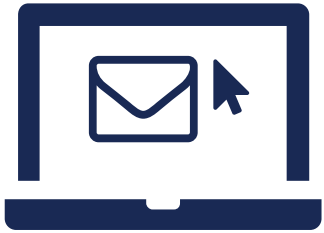
Launch

Exploit

Install

Callback

Email w/ Ransomware Payload



User Clicks a Malicious Link, Malvertising

Exploitation

Call to malicious Infrastructure

Ransomware Payload

Decryption key asymmetric exchange





Files inaccessible

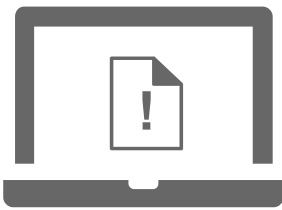
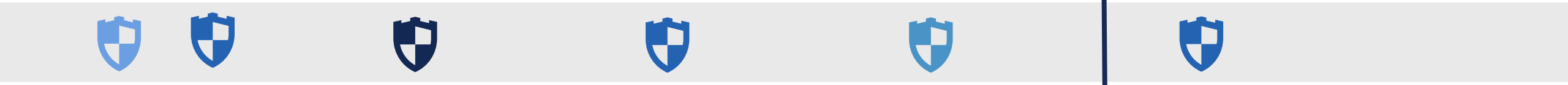


# Multi-layer defense that can improve TTD

Email w/ Ransomware Payload



-  Email Security
-  DNS Layer
-  Endpoint Security
-  Intrusion Prevention



User Clicks a Malicious Link, Malvertising

Exploitation

Call to malicious Infrastructure

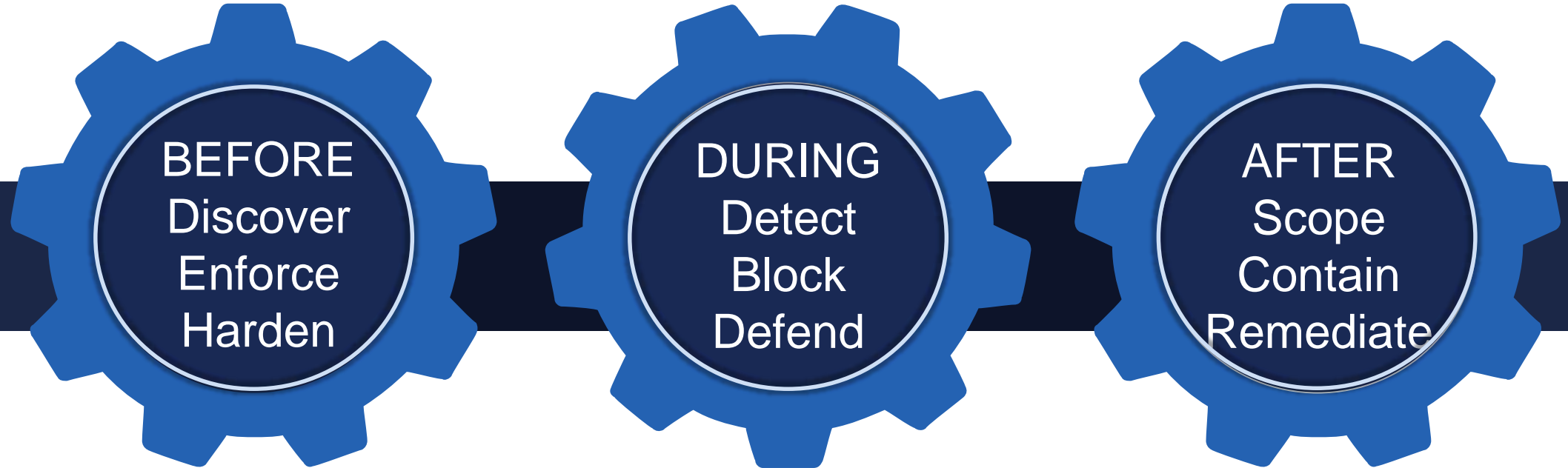
Ransomware Payload

Decryption key asymmetric exchange

Files inaccessible



# Protection after an attack is crucial to lowering TTD



Network



Endpoint



Mobile



Virtual



Cloud



Threat Intelligence

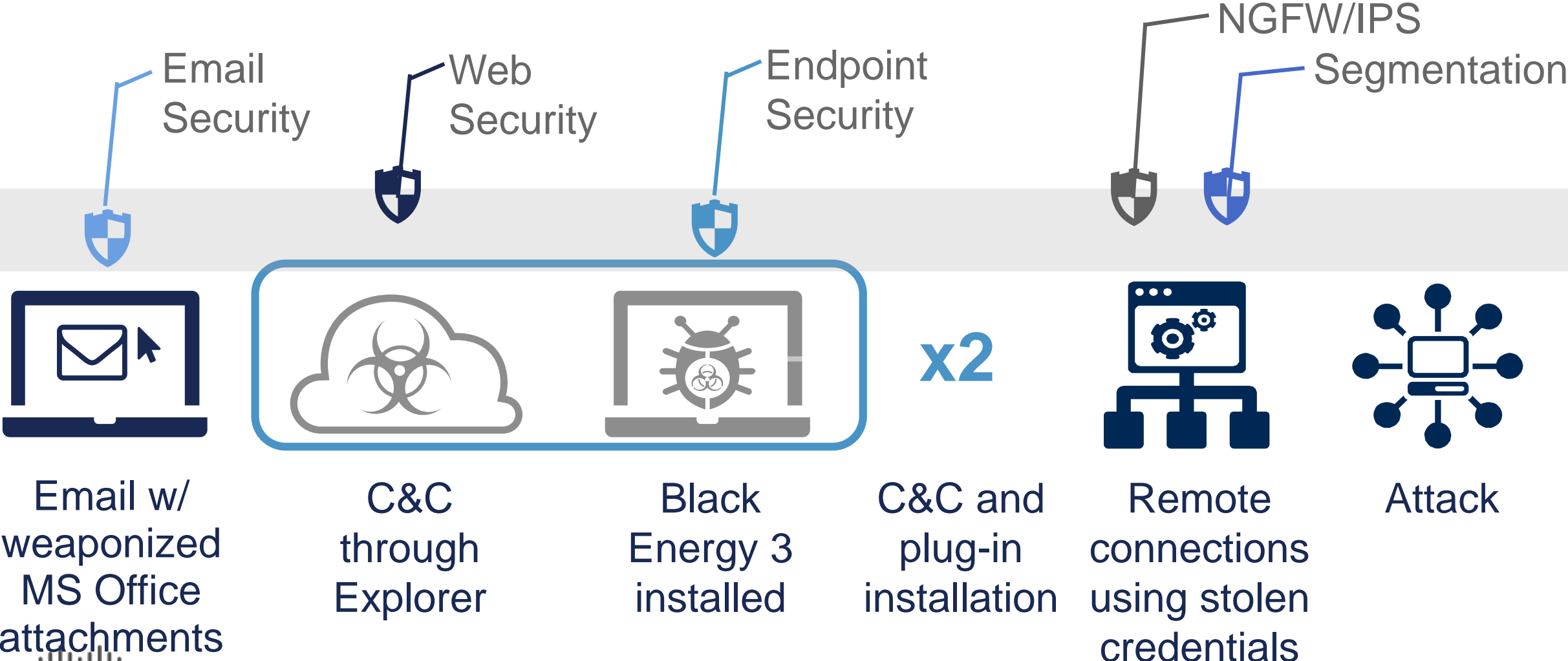


Point in Time



Continuous

# A multi-layer defense lowers TTD for other threats – like Black Energy



Email w/  
weaponized  
MS Office  
attachments

C&C  
through  
Explorer

Black  
Energy 3  
installed

x2

C&C and  
plug-in  
installation

Remote  
connections  
using stolen  
credentials

Attack



Protecting multiple attack vectors and 'after' an attack is more effective at lowering TTD than protecting early on in the kill chain

# Why are attackers so fast?

# Time to Patch: Vulnerable Endpoints Are Ripe Targets



# Don't ignore encryption

Adversaries hide their tracks in the encrypted traffic to evade detection.

	<b>HTTPS Malware Traffic Increase</b>	<b>% Increase</b>	<b>% Avg. HTTPS</b>
	<b>Advertisements</b>	<b>+9.27%</b>	<b>34.06%</b>
	<b>Search Engines and Portals</b>	<b>+8.58%</b>	<b>64.27%</b>
	<b>Chat and Instant Messaging</b>	<b>+8.23%</b>	<b>96.83%</b>



Technical considerations alone are not enough



# Combining people, processes and technology

Strategy (People)



Operations (Process)



Tactical (Technology)



# Ukraine National Center for Cybersecurity will support people, processes

National Cyber Security Strategy

National Coordination Center for Cybersecurity

## УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №96/2016

Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України"

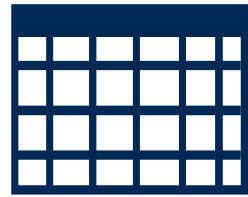


# How Cisco lowers Total Time to Detection

# More Effective Against Sophisticated Attacks

Much faster than most organizations discover breaches

100



vs



13

Industry Days

Cisco Hours

\*Source Cisco Midyear Security Report, 2016

# Integrated threat defense: sharing information to lower TTD



Event



Threat intel



Policy

# Unrivaled global threat research and intelligence



**100 TB Data  
Received**

**1.5 MILLION  
Malware Samples**

**600 BILLION  
Email Messages**

**16 BILLION  
Web Requests**



1110011 0110011 01010101 0110 100 000110 1010 0110 00  
1110011 0110011 10101110 10 10 101 0010 1000 0110 00  
1110011 0110011 101000 0110 00010100 10 1000101 011 010101



**24 · 7 · 365  
Operations**



**250+ Full Time Threat  
Intel Researchers**

**MILLIONS of Telemetry  
Agents**

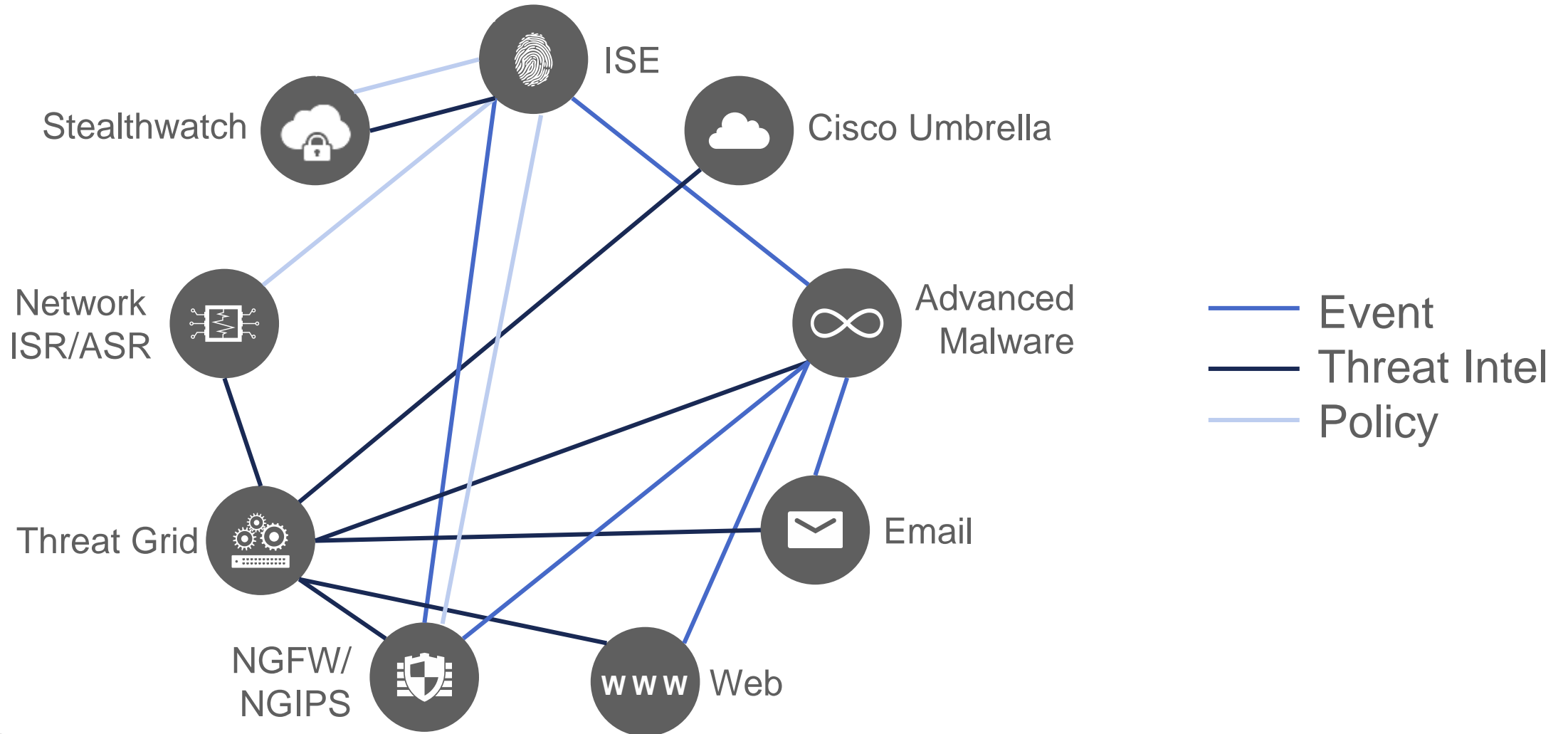
**4 Global Data Centers**

**Over 100 Threat  
Intelligence Partners**

# Threat Sharing Demo



# Product intercommunication across many attack vectors lowers TTD



# The minimum for lowering TTD

## People

Educate users about threats and best practices



## Process

Measure TTD

Basic hardening to resist malware and attacks

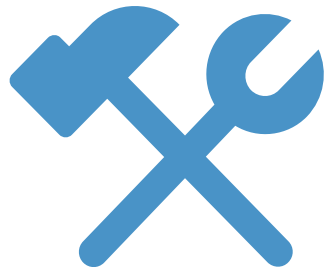
Develop an incident response plan

## Technology



Monitor network actively for evidence of compromise

What/how many/where are the devices on the network



“Carol of the Bells”

Rakhiv, Ukraine is the center of Europe

World’s first constitution

4<sup>th</sup> most educated country in the world

