RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

NOW MATTERS

SESSION ID: SPO3-R04

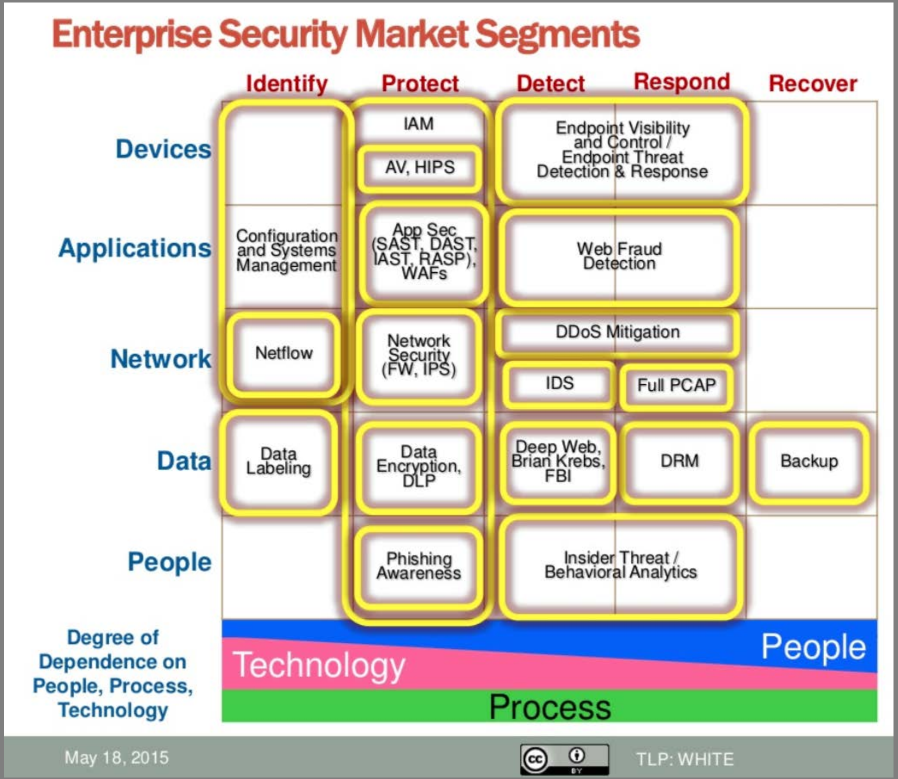
ENDPOINT SECURITY AND THE CLOUD: HOW TO APPLY PREDICTIVE ANALYTICS AND BIG DATA

Brian Gladstein

Cybersecurity Market Strategist
Carbon Black
@briangladstein

ASYMMETRIC WARFARE

IT’S THIS



Enterprise Security Market Segments

	Identify	Protect	Detect	Respond	Recover
Devices		IAM AV, HIPS	Endpoint Visibility and Control / Endpoint Threat Detection & Response		
Applications	Configuration and Systems Management	App Sec (SAST, DAST, IAST, RASP), WAFs	Web Fraud Detection		
Network	Netflow	Network Security (FW, IPS)	DDoS Mitigation IDS	Full PCAP	
Data	Data Labeling	Data Encryption, DLP	Deep Web, Brian Krebs, FBI	DRM	Backup
People		Phishing Awareness	Insider Threat / Behavioral Analytics		

Degree of Dependence on People, Process, Technology

Technology

People

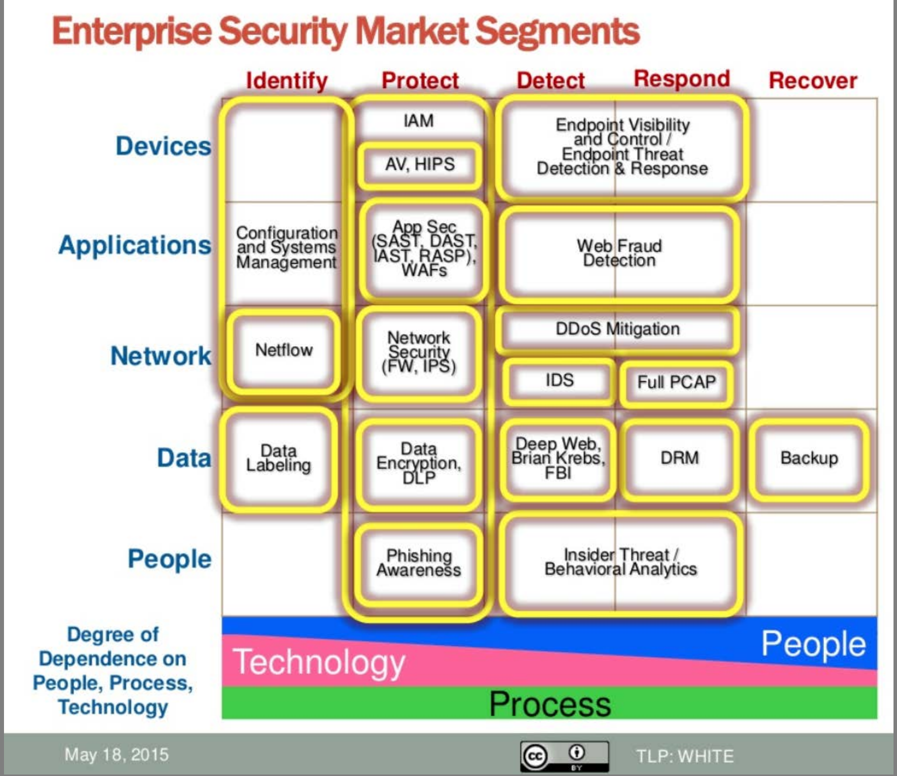
Process

May 18, 2015

TLP: WHITE

https://www.slideshare.net/sounilyu/understanding-the-cyber-security-vendor-landscape

VS THIS



Enterprise Security Market Segments

	Identify	Protect	Detect	Respond	Recover
Devices		IAM AV, HIPS	Endpoint Visibility and Control / Endpoint Threat Detection & Response		
Applications	Configuration and Systems Management	App Sec (SAST, DAST, IAST, RASP), WAFs	Web Fraud Detection		
Network	Netflow	Network Security (FW, IPS)	DDoS Mitigation IDS	Full PCAP	
Data	Data Labeling	Data Encryption, DLP	Deep Web, Brian Krebs, FBI	DRM	Backup
People		Phishing Awareness	Insider Threat / Behavioral Analytics		

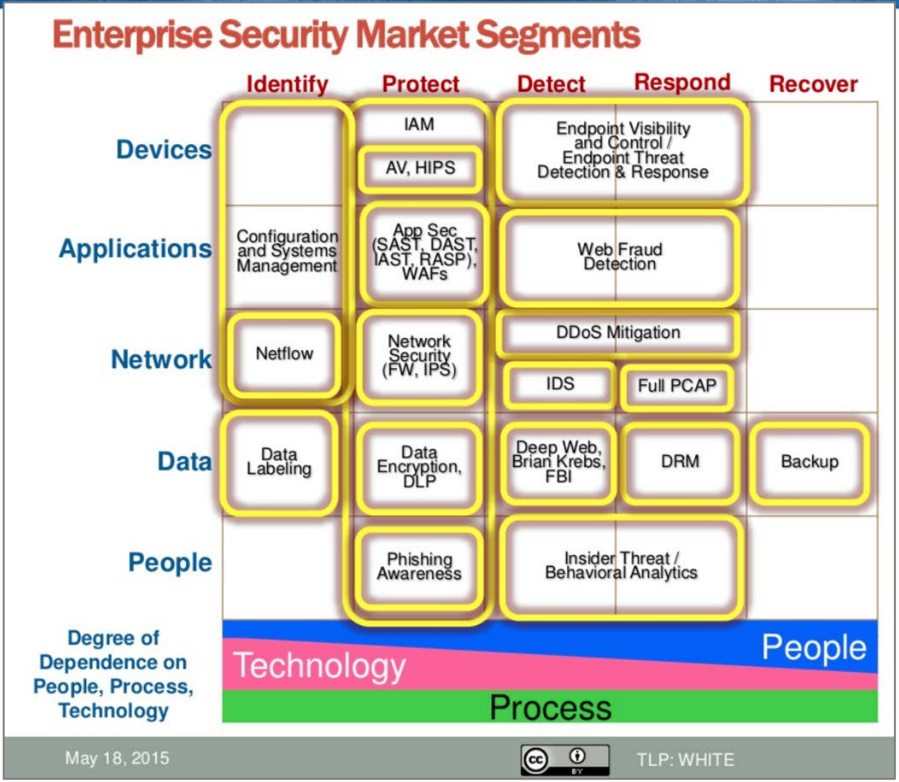
Degree of Dependence on People, Process, Technology

May 18, 2015

TLP: WHITE

OR IS IT?

ENDPOINT STACK PROBLEMS



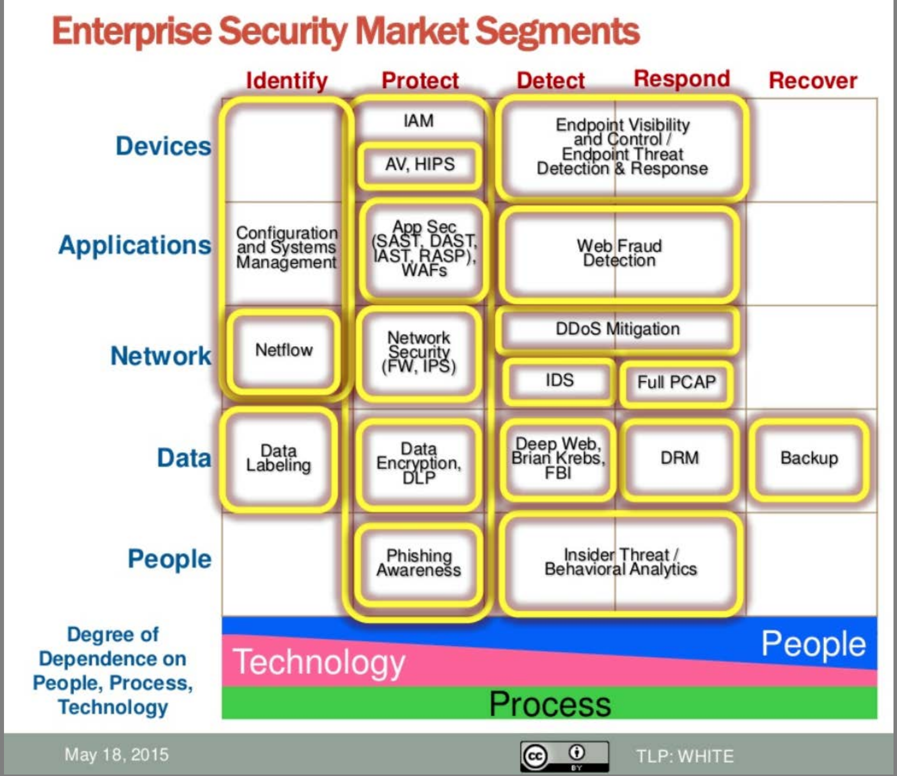
Enterprise Security Market Segments

	Identify	Protect	Detect	Respond	Recover
Devices		IAM AV, HIPS	Endpoint Visibility and Control / Endpoint Threat Detection & Response		
Applications	Configuration and Systems Management	App Sec (SAST, DAST, IAST, RASP), WAFs	Web Fraud Detection		
Network	Netflow	Network Security (FW, IPS)	DDoS Mitigation IDS	Full PCAP	
Data	Data Labeling	Data Encryption, DLP	Deep Web, Brian Krebs, FBI	DRM	Backup
People		Phishing Awareness	Insider Threat / Behavioral Analytics		

Degree of Dependence on People, Process, Technology

May 18, 2015 TLP: WHITE

- Outdated technology
- Too many tools, don’t work together
- Visibility
- Vulnerabilities, patching, updates
- Resource usage & performance
- The end-user
- Skills needed to operate
- Learning & getting better



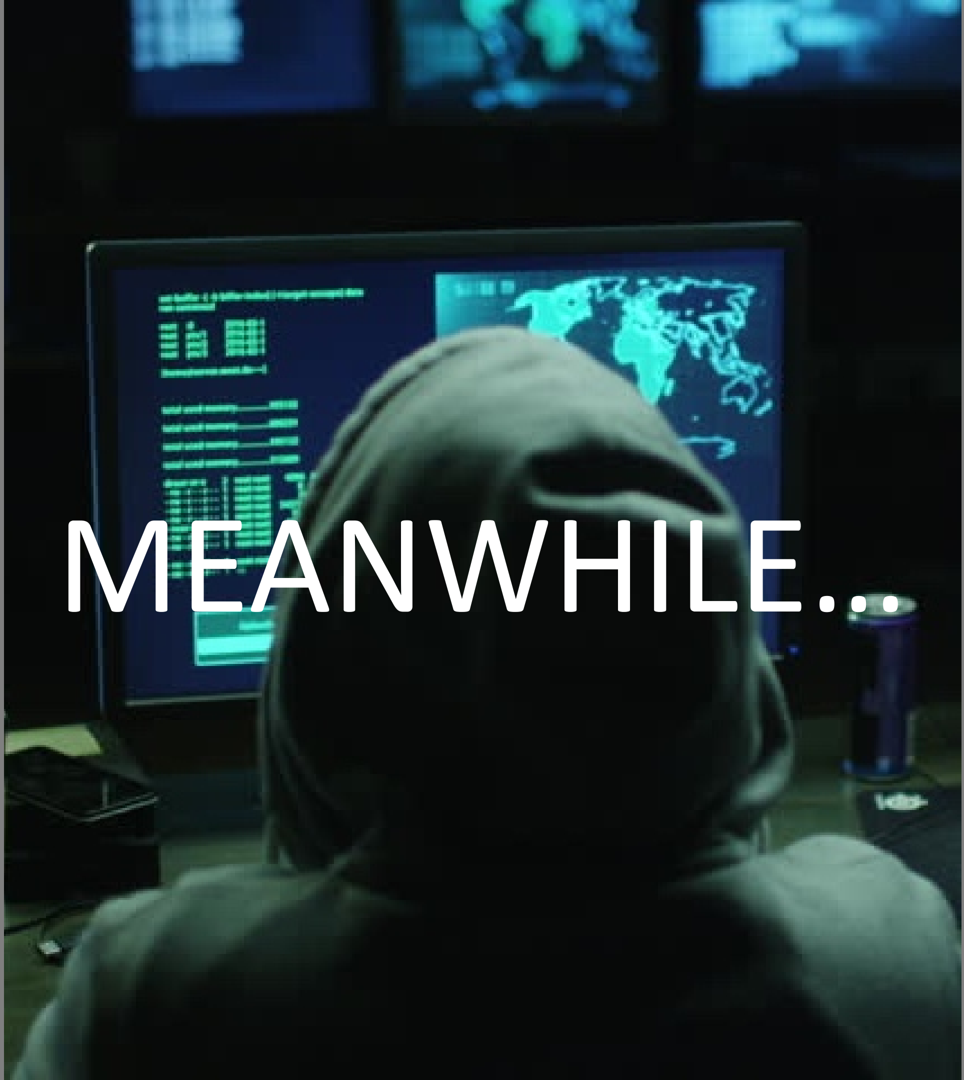
Enterprise Security Market Segments

	Identify	Protect	Detect	Respond	Recover
Devices		IAM AV, HIPS	Endpoint Visibility and Control / Endpoint Threat Detection & Response		
Applications	Configuration and Systems Management	App Sec (SAST, DAST, IAST, RASP), WAFs	Web Fraud Detection		
Network	Netflow	Network Security (FW, IPS)	DDoS Mitigation IDS	Full PCAP	
Data	Data Labeling	Data Encryption, DLP	Deep Web, Brian Krebs, FBI	DRM	Backup
People		Phishing Awareness	Insider Threat / Behavioral Analytics		

Degree of Dependence on People, Process, Technology

May 18, 2015

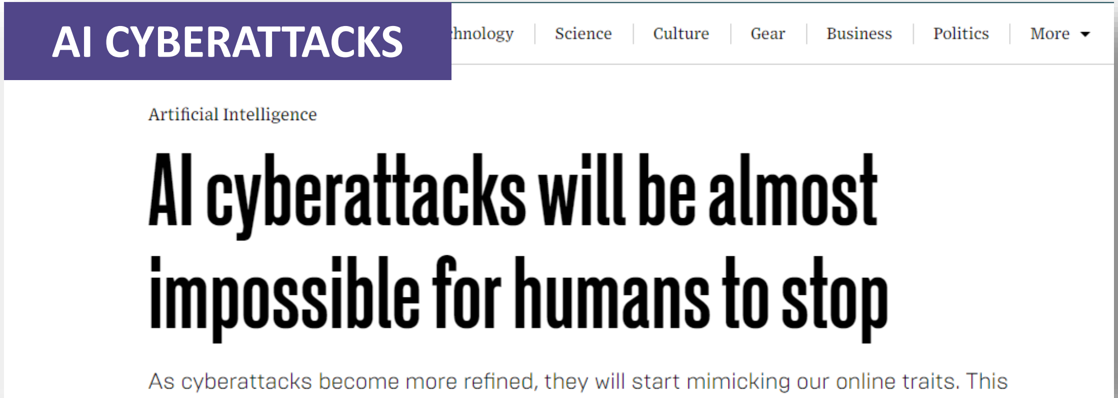
TLP: WHITE



MEANWHILE...

ATTACKERS ARE INNOVATING

AI CYBERATTACKS

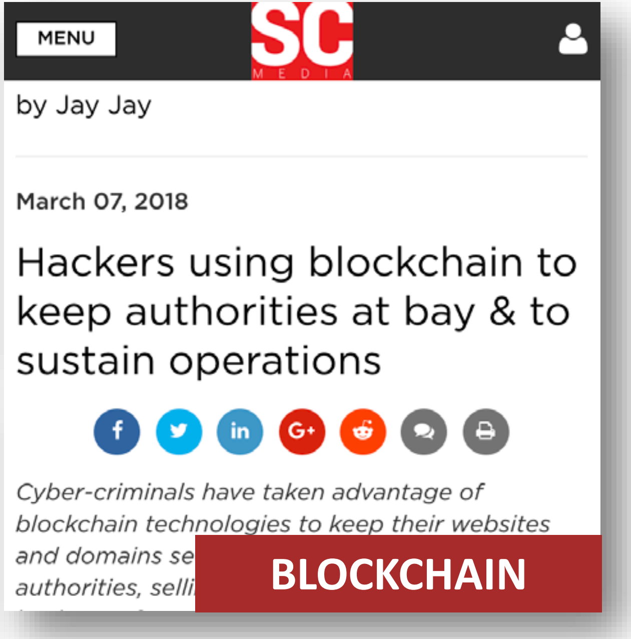


hnology | Science | Culture | Gear | Business | Politics | More

Artificial Intelligence

AI cyberattacks will be almost impossible for humans to stop

As cyberattacks become more refined, they will start mimicking our online traits. This



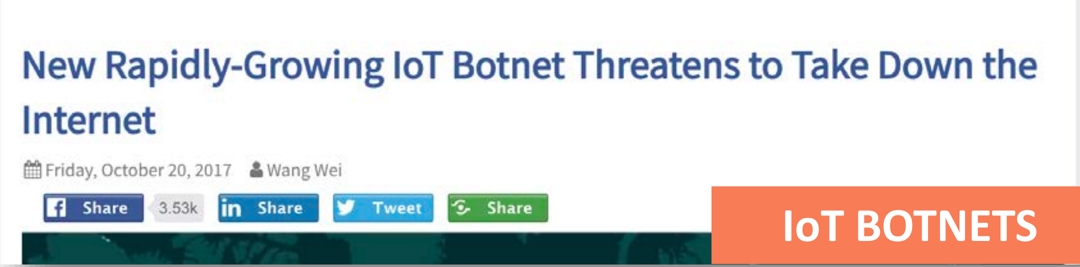
by Jay Jay

March 07, 2018

Hackers using blockchain to keep authorities at bay & to sustain operations

Cyber-criminals have taken advantage of blockchain technologies to keep their websites and domains se authorities, selli

BLOCKCHAIN



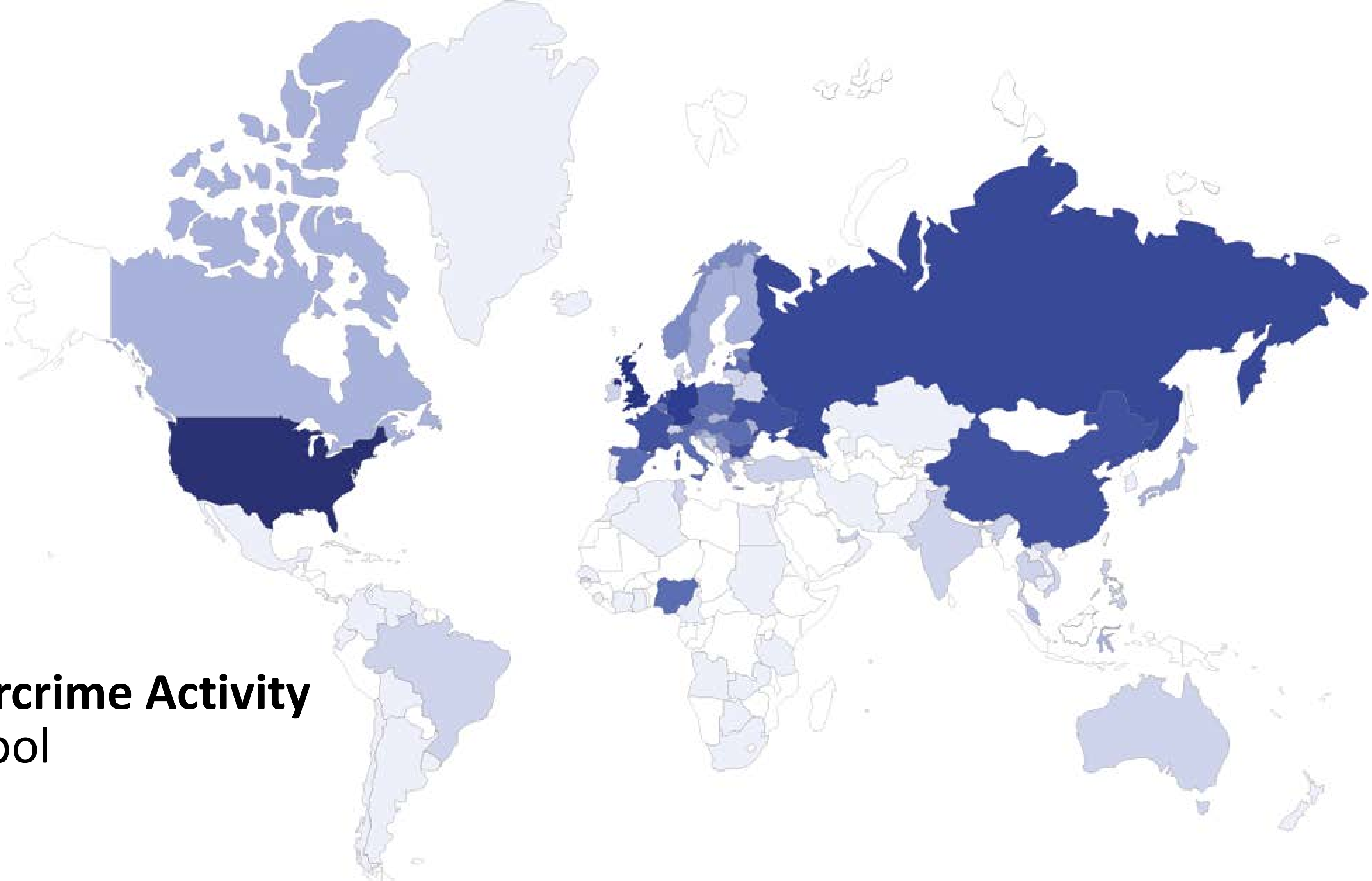
New Rapidly-Growing IoT Botnet Threatens to Take Down the Internet

Friday, October 20, 2017 Wang Wei

IoT BOTNETS

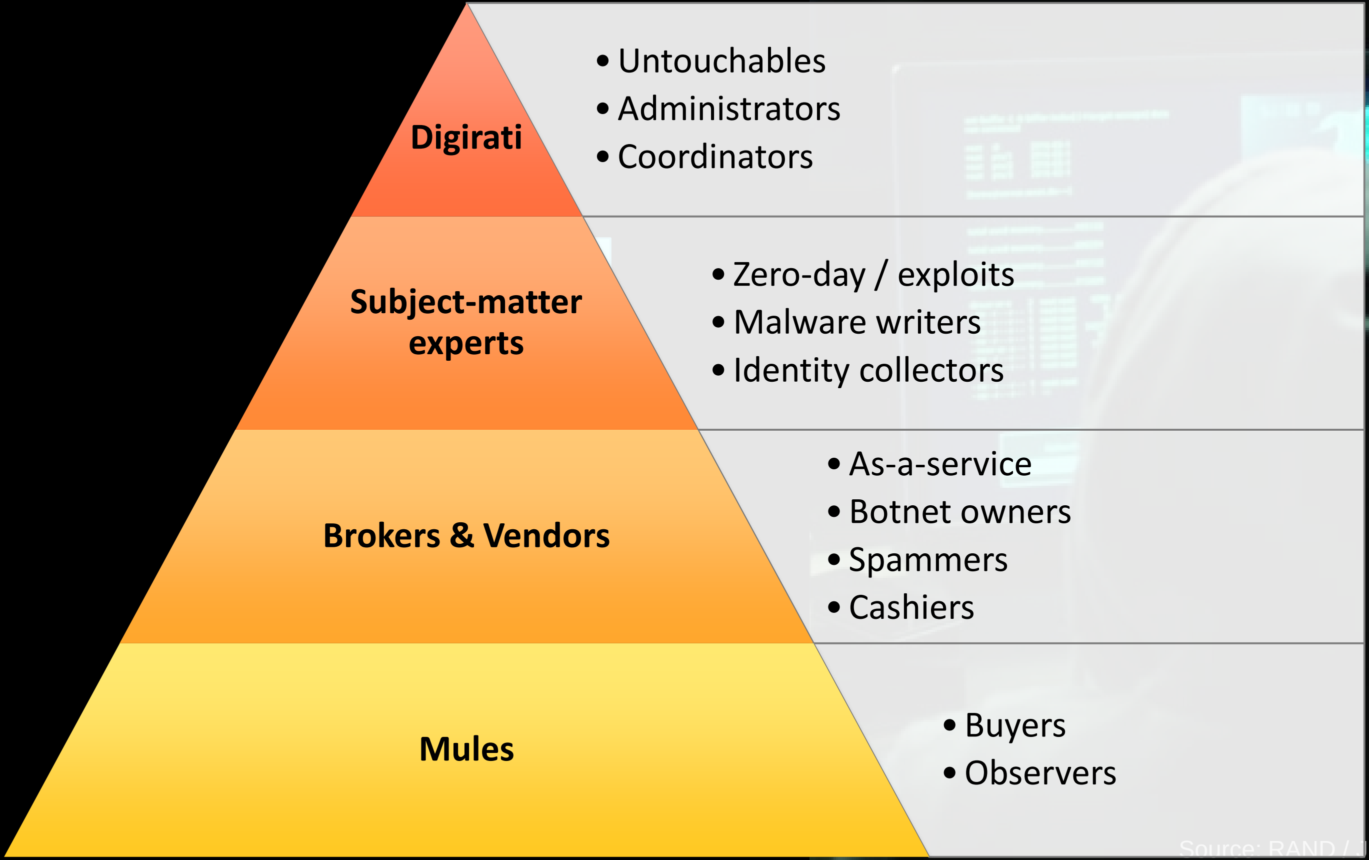
GERASIMOV DOCTRINE

Blurring of the lines between war and peace… Nonmilitary means of achieving military and strategic goals have grown and, in many cases, exceeded the power of weapons in their effectiveness.



Cybercrime Activity
Europol

IT’S AN ECONOMY



Digirati

- Untouchables
- Administrators
- Coordinators

Subject-matter experts

- Zero-day / exploits
- Malware writers
- Identity collectors

Brokers & Vendors

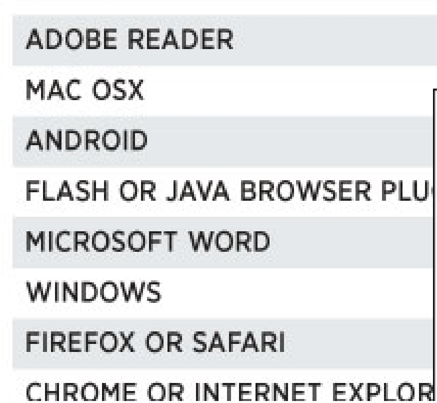
- As-a-service
- Botnet owners
- Spammers
- Cashiers

Mules

- Buyers
- Observers

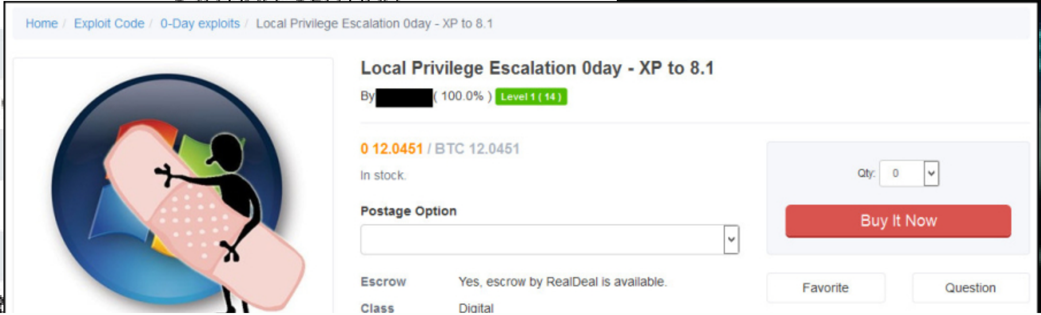
Source: RAND / Juniper

DRIVEN BY SPECIALIZATION



ADOBE READER	$5,000-$30,000
MAC OSX	$20,000-$50,000
ANDROID	
FLASH OR JAVA BROWSER PLU	
MICROSOFT WORD	
WINDOWS	
FIREFOX OR SAFARI	
CHROME OR INTERNET EXPLOR	

Approximate pricing, 2012
Source: Forbes.com



Home / Exploit Code / 0-Day exploits / Local Privilege Escalation 0day - XP to 8.1

Local Privilege Escalation 0day - XP to 8.1

By [redacted] (100.0%) Level 1 (14)

0 12.0451 / BTC 12.0451

In stock.

Postage Option

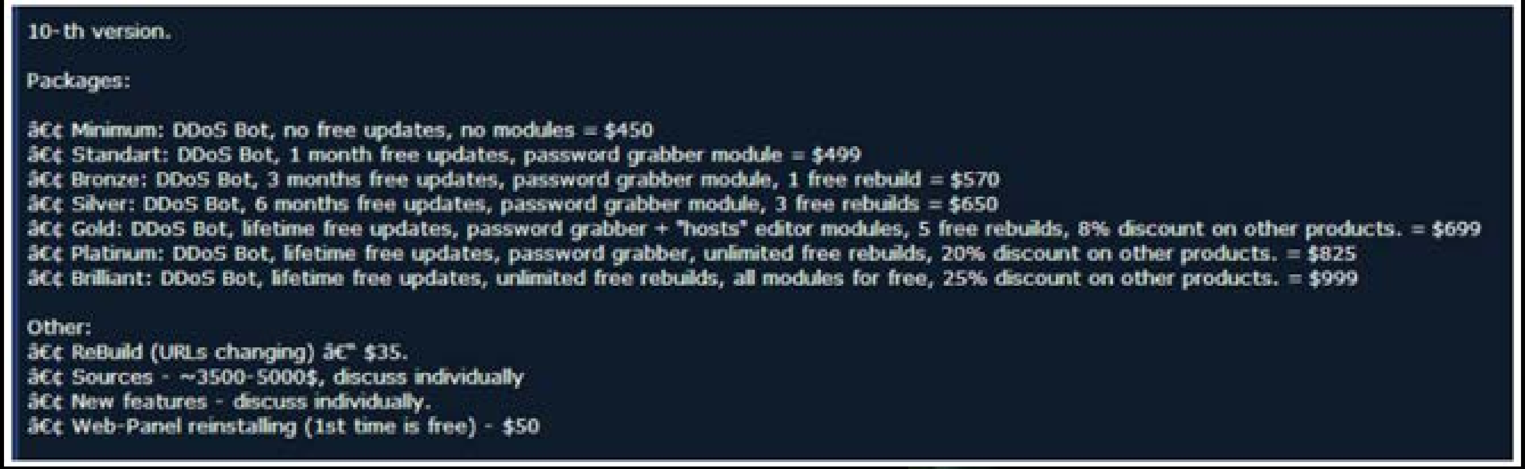
Qty: 0

Buy It Now
Favorite
Question

Escrow Yes, escrow by RealDeal is available.

Class Digital

Windows Zero-day
Source: Forbes.com



```
10-th version.

Packages:

â€¢ Minimum: DDoS Bot, no free updates, no modules = $450
â€¢ Standart: DDoS Bot, 1 month free updates, password grabber module = $499
â€¢ Bronze: DDoS Bot, 3 months free updates, password grabber module, 1 free rebuild = $570
â€¢ Silver: DDoS Bot, 6 months free updates, password grabber module, 3 free rebuilds = $650
â€¢ Gold: DDoS Bot, lifetime free updates, password grabber + "hosts" editor modules, 5 free rebuilds, 8% discount on other products. = $699
â€¢ Platinum: DDoS Bot, lifetime free updates, password grabber, unlimited free rebuilds, 20% discount on other products. = $825
â€¢ Brilliant: DDoS Bot, lifetime free updates, unlimited free rebuilds, all modules for free, 25% discount on other products. = $999

Other:
â€¢ ReBuild (URLs changing) â€" $35.
â€¢ Sources - ~3500-5000$, discuss individually
â€¢ New features - discuss individually.
â€¢ Web-Panel reinstalling (1st time is free) - $50
```

Botnet Rentals
Source: Infosec Institute

ATTACKERS ARE OUT-INNOVATING US

- Sustained, targeted attacks
- Purpose-built payloads
- Colonization of infrastructure
- Zero day vulnerability development for applications
- Drops, logs, translation, laundering – all for sale
- Destructive attacks as a service

WE NEED TO LEARN FROM THE BEST

THE ADVERSARY ALREADY HAS A FOOTPRINT

- Real-time situational awareness
- Continuous monitoring
- Dwell time is your enemy

SHIFTING SECURITY APPROACH

THE OLD WAY

ENDPOINT → Prevention

NETWORK → Detection & Response

SHIFTING SECURITY APPROACH

WATCH & RECORD EVERYTHING

THE NEW WAY

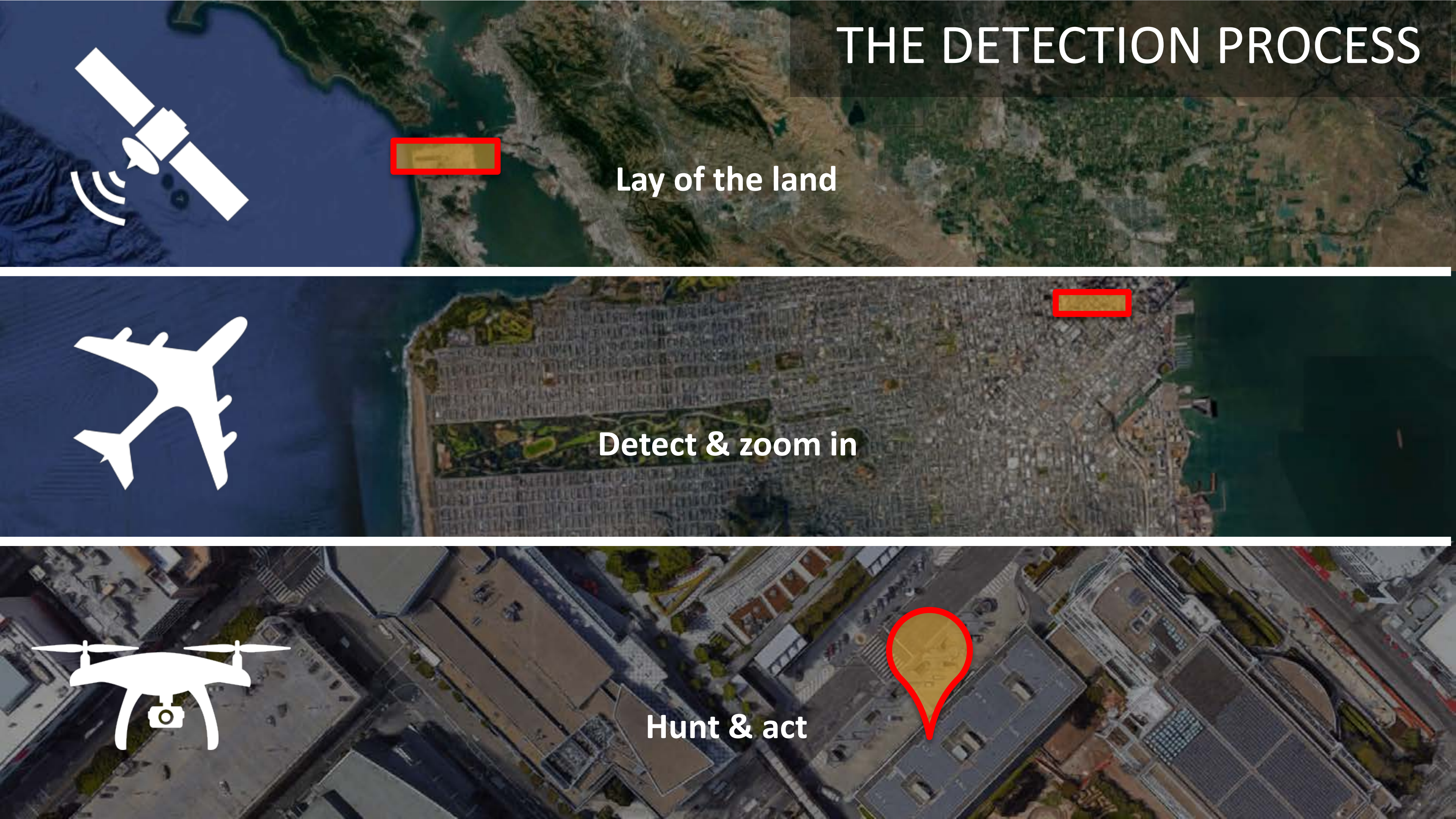
ENDPOINT + NETWORK

⬇

Prediction, Prevention,

Detection, Response

THE DETECTION PROCESS

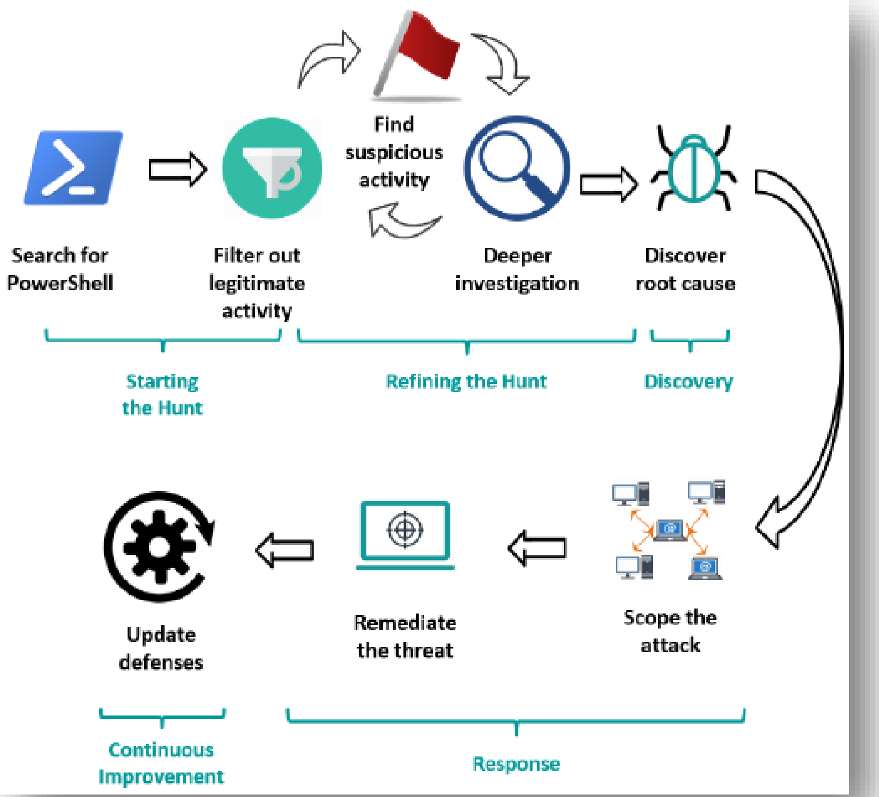


Lay of the land

Detect & zoom in

Hunt & act

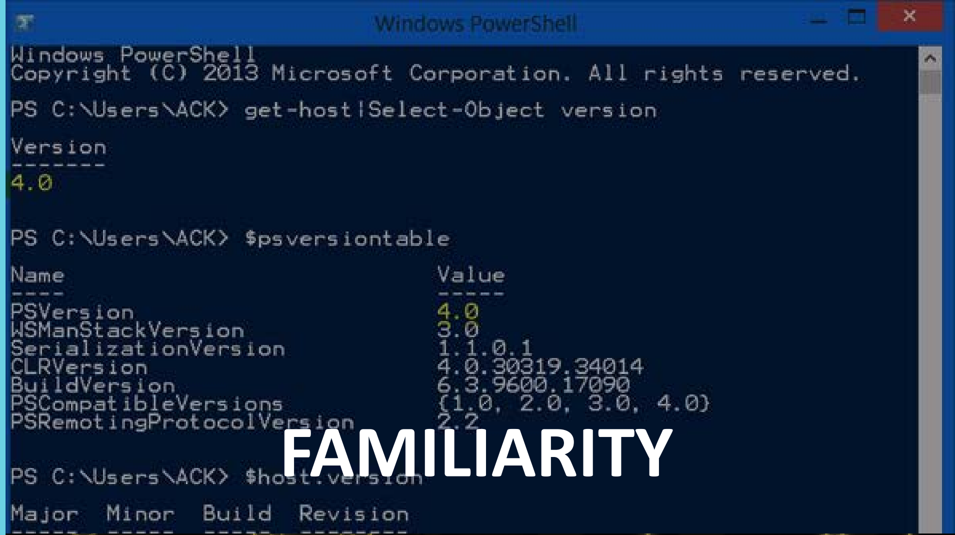
THREAT HUNTING PROCESS



USE TECHNOLOGY TO:

- Automate
- Accelerate
- Broaden coverage
- Increase effectiveness
- Fix

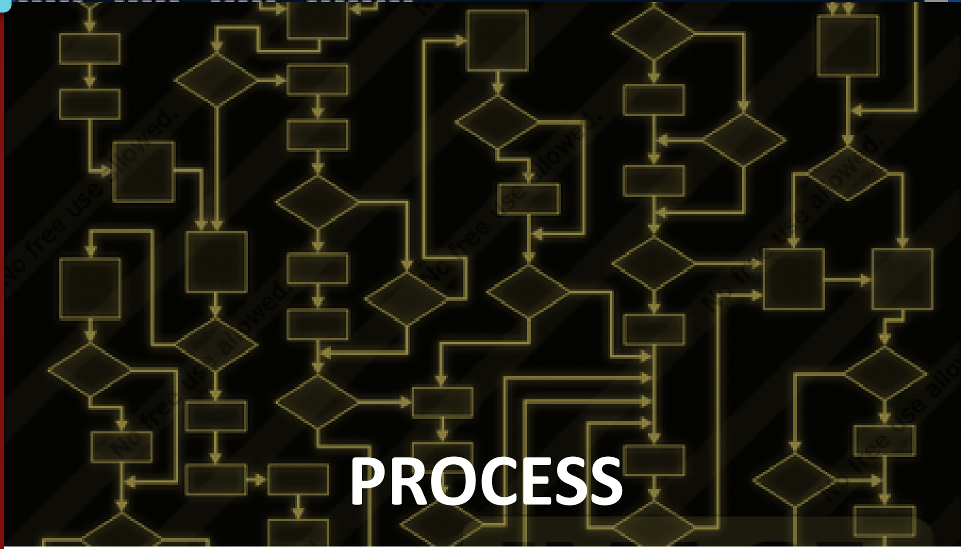
INSTINCTS



```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\ACK> get-host|Select-Object version

Version
-------
4.0


PS C:\Users\ACK> $psversiontable

Name                           Value
----                           -----
PSVersion                      4.0
WSManStackVersion              3.0
SerializationVersion           1.1.0.1
CLRVersion                     4.0.30319.34014
BuildVersion                   6.3.9600.17090
PSCompatibleVersions           {1.0, 2.0, 3.0, 4.0}
PSRemotingProtocolVersion      2.2


PS C:\Users\ACK> $host.version

Major  Minor  Build  Revision
-----  -----  -----  --------
```

FAMILIARITY

THREAT INTELLIGENCE



PROCESS

WHAT DO THREAT HUNTERS LOOK FOR?

persistence

memory scraping

suspicious downloads

password-cracking attempts

anomalous behavior

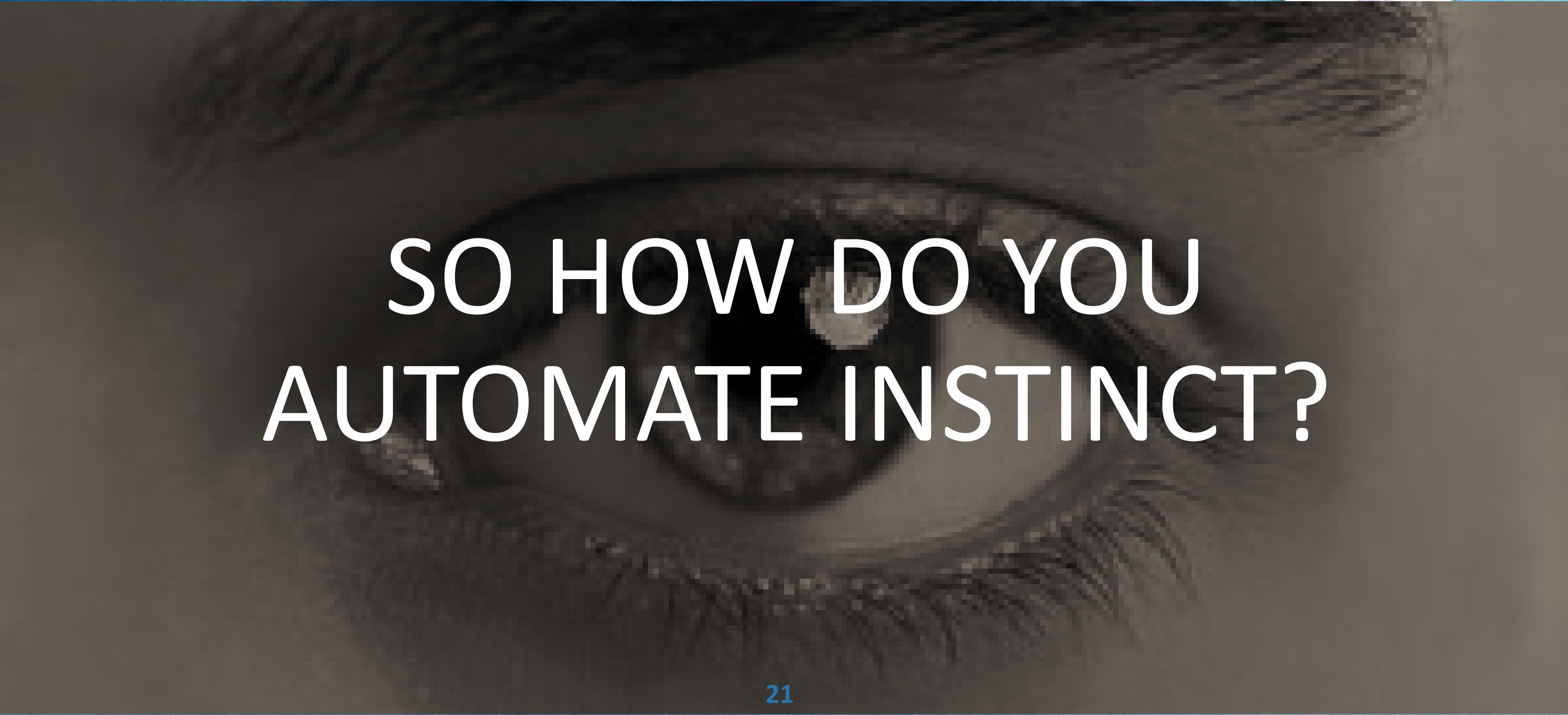
unexplained data

code injection

new network connections

access to sensitive files

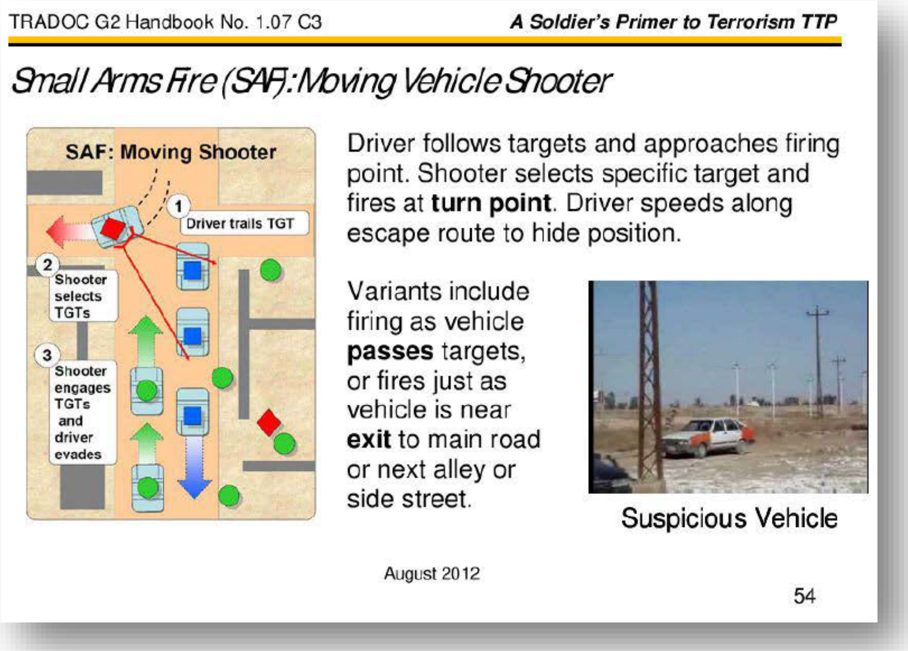
WHAT DO THREAT HUNTERS LOOK FOR?



SO HOW DO YOU AUTOMATE INSTINCT?

TTP: TACTIC, TECHNIQUE, PROCEDURE

The role of TTPs in terrorism analysis is to identify individual patterns of behavior … and to examine and categorize more general tactics and weapons used…



TRADOC G2 Handbook No. 1.07 C3 *A Soldier's Primer to Terrorism TTP*

Small Arms Fire (SAF): Moving Vehicle Shooter

SAF: Moving Shooter
1 Driver trails TGT
2 Shooter selects TGTs
3 Shooter engages TGTs and driver evades

Driver follows targets and approaches firing point. Shooter selects specific target and fires at **turn point**. Driver speeds along escape route to hide position.

Variants include firing as vehicle **passes** targets, or fires just as vehicle is near **exit** to main road or next alley or side street.

Suspicious Vehicle

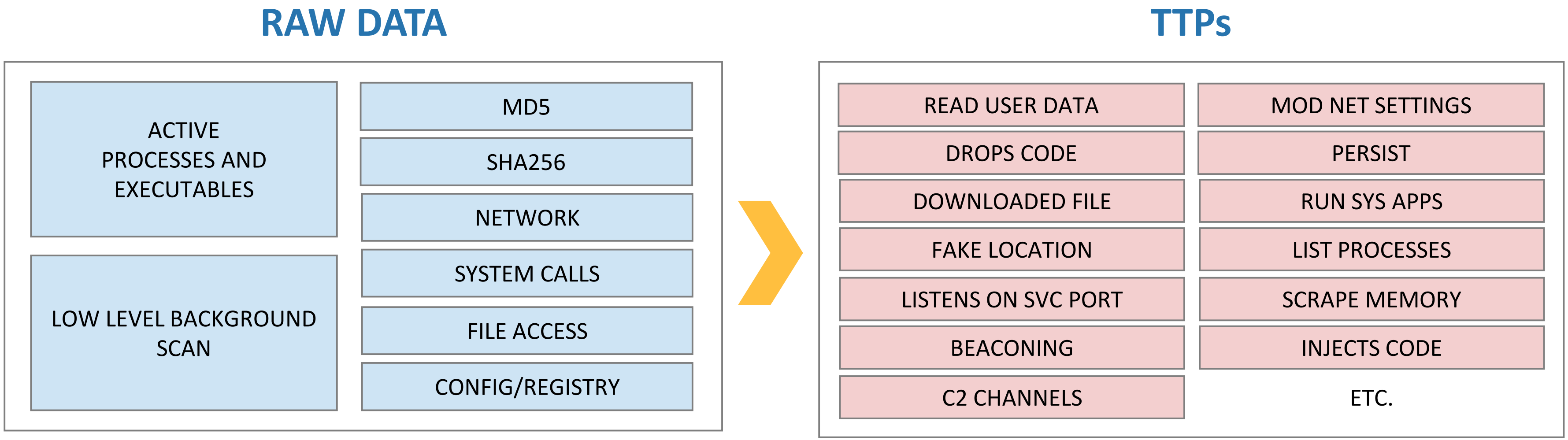
August 2012

54

https://en.wikipedia.org/wiki/Terrorist_Tactics,_Techniques,_and_Procedures

https://publicintelligence.net/usarmy-terrorism-ttps/

TTPs IN CYBER



RAW DATA

ACTIVE PROCESSES AND EXECUTABLES

LOW LEVEL BACKGROUND SCAN

MD5

SHA256

NETWORK

SYSTEM CALLS

FILE ACCESS

CONFIG/REGISTRY

TTPs

READ USER DATA

DROPS CODE

DOWNLOADED FILE

FAKE LOCATION

LISTENS ON SVC PORT

BEACONING

C2 CHANNELS

MOD NET SETTINGS

PERSIST

RUN SYS APPS

LIST PROCESSES

SCRAPE MEMORY

INJECTS CODE

ETC.

A TTP EXAMPLE: PERSISTENCE

TTP: PERSISTENCE

Techniques for maintaining access to a compromised system even after rebooting or remediation

PERSISTENCE

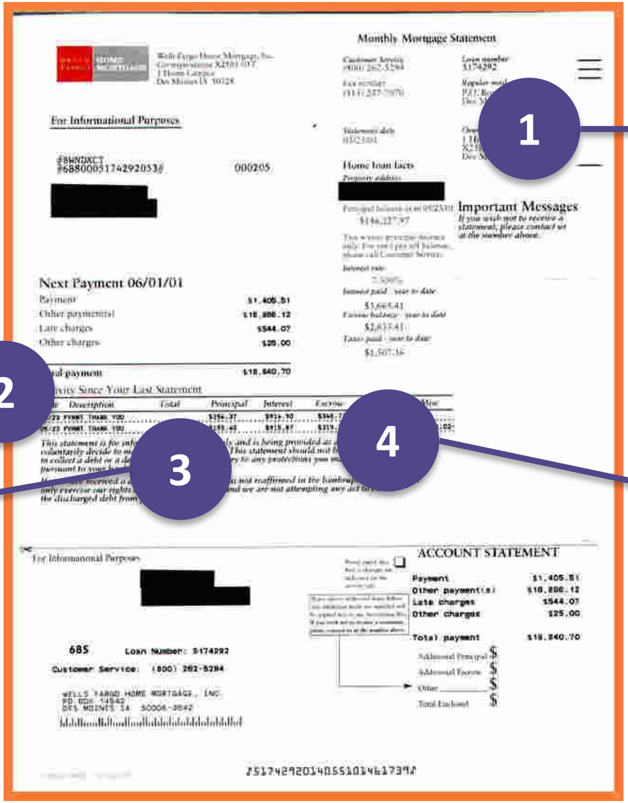
```
C:\autorun.inf
C:\Windows\System32\Tasks
HKEY_CURRENT_USER\...\User Shell Folders
HKEY_LOCAL_MACHINE\SYSTEM\...\service
HKEY_LOCAL_MACHINE\SOFTWARE\...\Notify
HKEY_LOCAL_MACHINE\SOFTWARE\...\RunOnce
... many, many more ...
```

A SAMPLING OF THE 200+ TTPs

FILE SYSTEM	NETWORK	PROCESS	SYSTEM SECURITY	USER INPUT
CREATE/MODIFY EXECUTABLE FILES	MODIFY NETWORK SETTINGS	PLUGIN INJECTION	DISABLE SECURITY SOFTWARE	TAKE SCREENSHOTS
READ USER DATA, (CAL, EMAIL, etc.)	C2 CHANNELS	KILL ANOTHER PROCESS	HARVEST PASSWORDS	READ FROM CLIPBOARD
PERSISTENCE	BEACONING	MEMORY SCRAPING	MODIFY CONFIGURATION	ENABLE MIC/WEBCAM
DOWNLOAD FILE FROM EMAILED URL	COMMUNICATE WITH LOW REP SITE	PRIVILEGE ESCALATION	MODIFY REGISTRY	CAPTURE KEYSTROKES

HOW TO THINK ABOUT TTPs

#RSAC



Monthly Mortgage Statement

Wells Fargo Home Mortgage, Inc.
Correspondence X2501-01T
1 Home Campus
Des Moines IA 50328

Customer Service
(800) 262-5294

Fax number
(515) 237-7070

Loan number
5174292

Regular mail
P.O. Bo[illegible]
Des M[illegible]

Statement date
05/23/01

Ov[illegible]
1 H[illegible]
X23[illegible]
Des M[illegible]

For Informational Purposes

#BWNDXCT
#6880005174292053#

000205

[redacted]

Home loan facts
Property address
[redacted]

Principal balance as of 05/23/01
$146,227.97

This is your principal balance only. For your pay-off balance, please call Customer Service.

Interest rate
7.500%

Interest paid - year to date
$3,665.41

Escrow balance - year to date
$2,637.41

Taxes paid - year to date
$1,507.16

Important Messages
If you wish not to receive a statement, please contact us at the number above.

Next Payment 06/01/01

Payment	$1,405.51
Other payment(s)	$16,886.12
Late charges	$544.07
Other charges	$25.00
[illegible]al payment	$18,860.70

[illegible]ivity Since Your Last Statement

[illegible]	Description	Total	Principal	Interest	Escrow	[illegible]	Misc
[illegible]/23	PYMNT THANK YOU		$256.37	$914.70	$346.7[illegible]	[illegible]	[illegible]
05/23	PYMNT THANK YOU		$155.40	$915.67	$319.[illegible]	[illegible]	[illegible]102

This statement is for info[illegible] [illegible]ly and is being provided as a[illegible] voluntarily decide to m[illegible] This statement should not b[illegible] to collect a debt or a de[illegible] [illegible]ry to any protections you m[illegible] pursuant to your ba[illegible]

If [illegible] received a d[illegible] [illegible]s not reaffirmed in the bankrup[illegible] only exercise our rights [illegible] and we are not attempting any act to [illegible] the discharged debt from [illegible]

For Informational Purposes

[redacted]

ACCOUNT STATEMENT

[illegible] □

Payment	$1,405.51
Other payment(s)	$16,886.12
Late charges	$544.07
Other charges	$25.00
Total payment	$18,860.70
Additional Principal	$
Additional Escrow	$
Other	$
Total Enclosed	$

685 Loan Number: 5174292

Customer Service: (800) 262-5294

WELLS FARGO HOME MORTGAGE, INC.
PO BOX 14542
DES MOINES IA 50306-3542

⑆5174292014055101461739⑈

1 Mismatched personal info

2 Making a purchase in a strange place

3 Luxury items

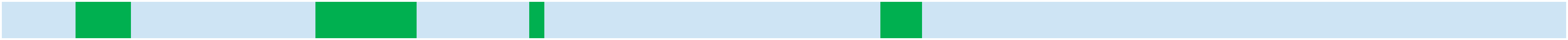
4 Small purchase followed by large purchase

Carbon Black.

RSAConference2018

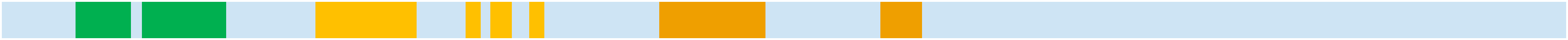
APPLYING TTPs TO ENDPOINT ACTIVITY

EVENT SEQUENCE 1 – NORMAL ACTIVITY



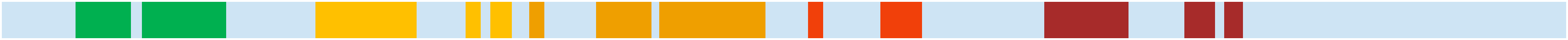
ASSESSMENT: LOW RISK

EVENT SEQUENCE 2 – SUSPICIOUS ACTIVITY



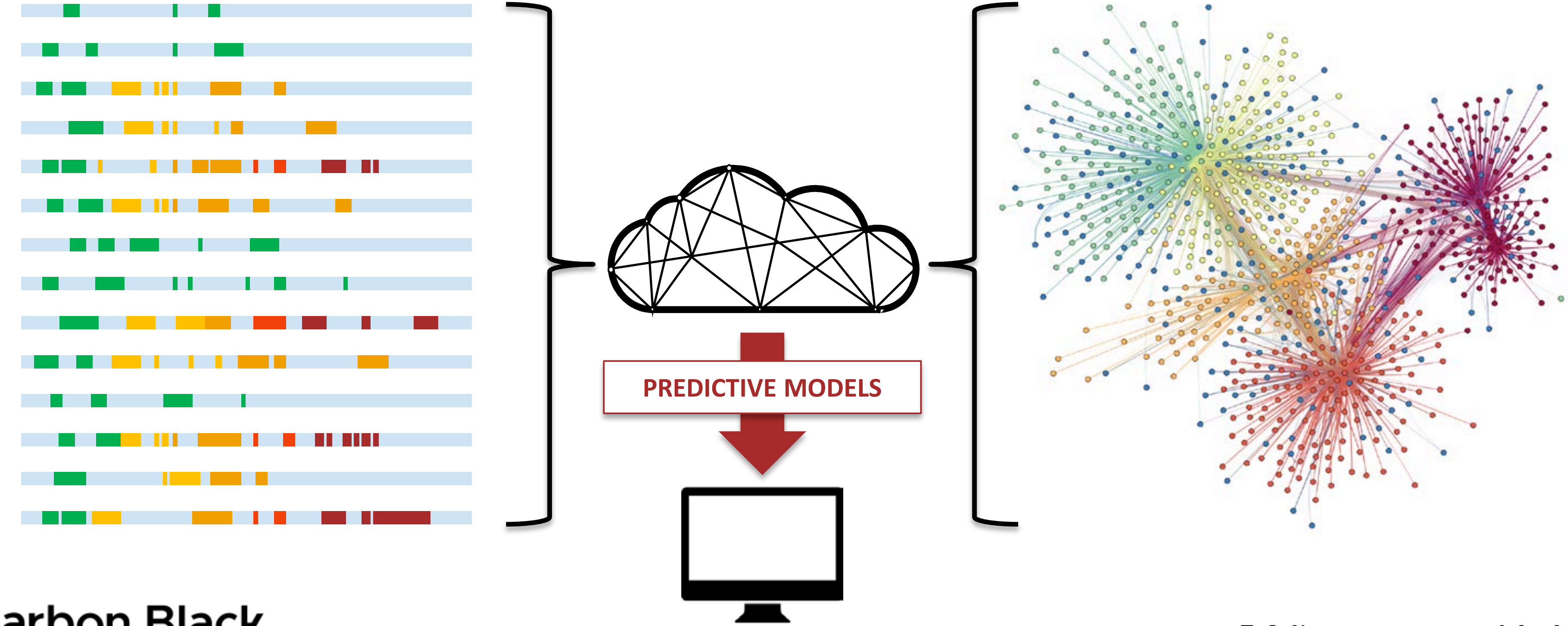
ASSESSMENT: MEDIUM RISK

EVENT SEQUENCE 3 – MALICIOUS ACTIVITY



ASSESSMENT: HIGH RISK

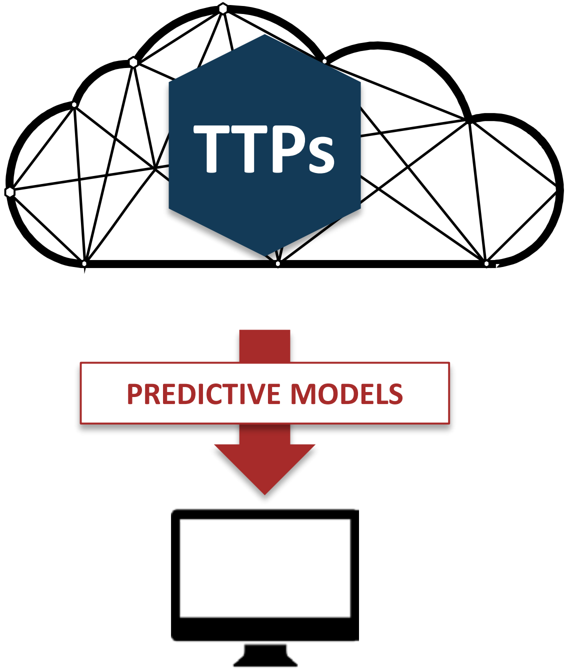
SCALING TTPs WITH BIG DATA & ANALYTICS



PREDICTIVE MODELS

FEEDING THE BIG DATA MACHINE

- Threat intelligence
- Threat research
- Community detection

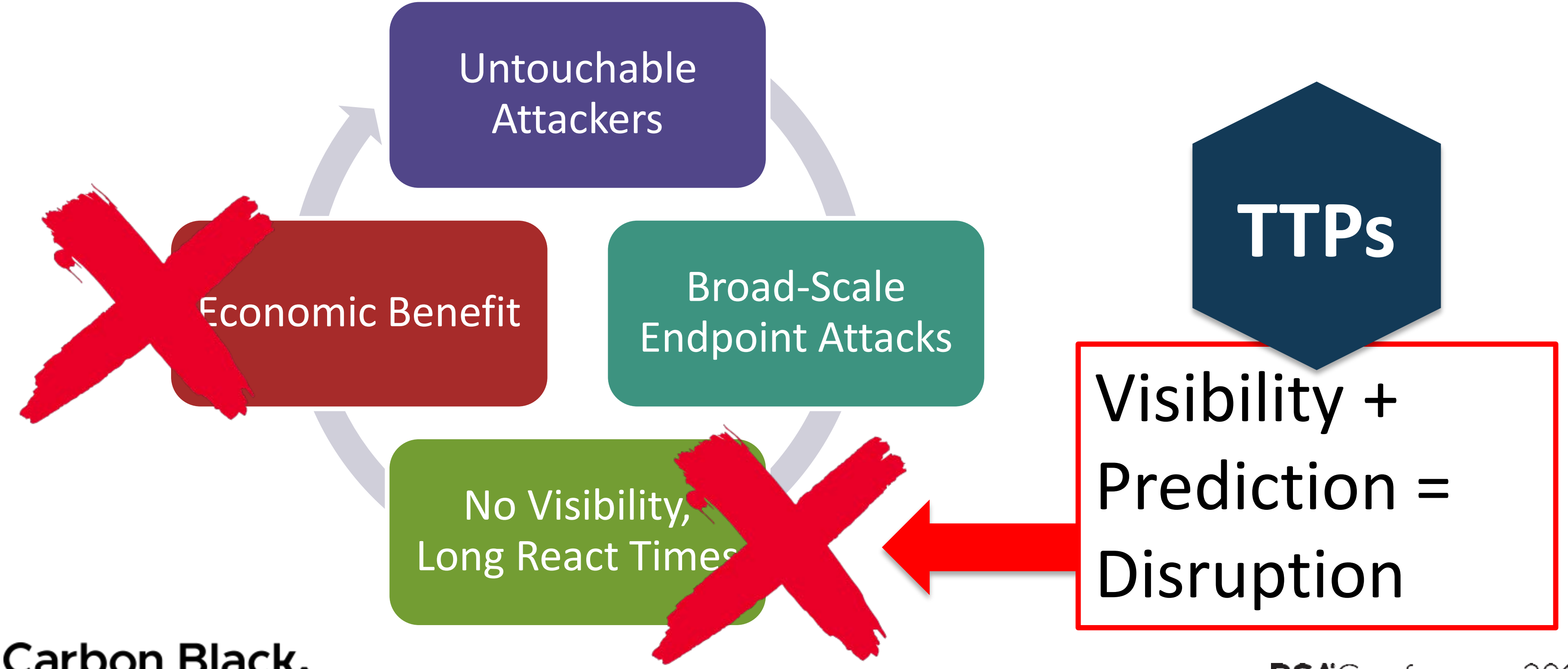


TTPs

PREDICTIVE MODELS

- Unfiltered Endpoint Data

DISRUPTING THE DIGIRATI CYCLE



Visibility + Prediction = Disruption

SUMMARY

- Attackers are out-innovating the defenders
- The best defenders combine technology with human instinct
- TTPs capture what threat hunters do and automate it
- Predictive security achieved through TTP-based detection at scale

PUTTING TTPs INTO PRACTICE

- Next week you should:
  - Assess the capabilities of your endpoint security products
  - Assess how you are using endpoint data in security operations
- In the first three months following this presentation you should:
  - Evaluate products that provide visibility to endpoints
  - Plan to converge prevention, detection, and response
- Within six months you should:
  - Implement next-generation endpoint security & threat hunting
  - Contribute to threat communities & cloud analytics

THANK YOU!

Brian Gladstein
Cybersecurity Market Strategist
Carbon Black
@briangladstein
briangladstein@carbonblack.com
(781) 820-2654