



BIG Data gone small – The Next Generation of Endpoint Protection

Eran Ashkenazi

VP of Services & Field Operations



©Copyright 2015 Sentinel Labs Inc. Business Confidential. Not for distribution.

Next Generation Endpoint Protection



Founded
1/2013



Employees
50+



Customers
50+
Tech
Energy
Pharma
Financial

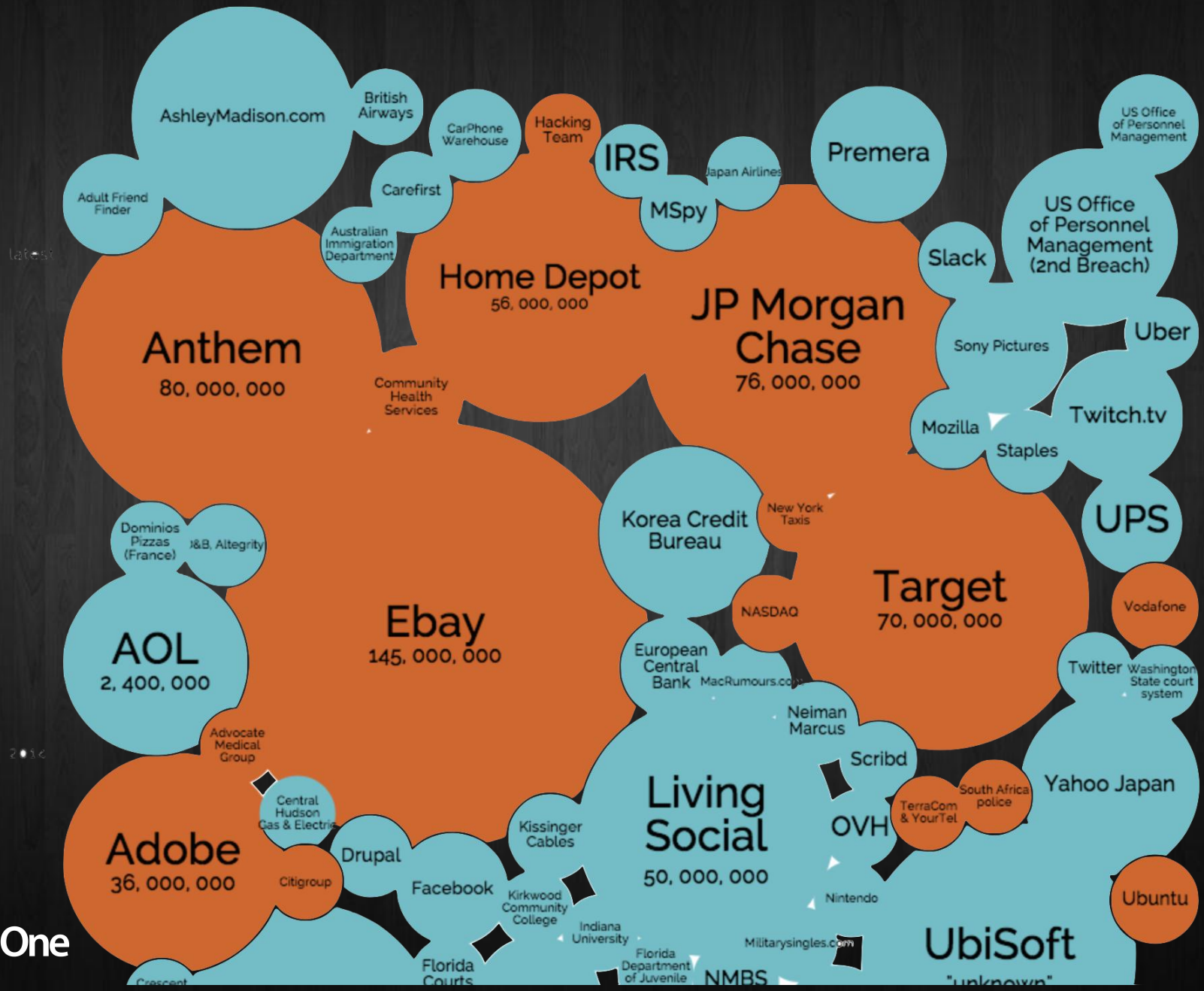


Raised
\$14.5M
Tiger Global
Accel Partners
Data Collective
Granite Hill



Offices
CA
ISRL
HQ
R&D
Mountain View
Tel-Aviv

TOP BREACHES & RECORDS STOLEN (2014-2015)



GLOBAL THREATS

Existing Solutions are Not Enough

The IT Enterprise Market Sees More Than

1,000,000,000

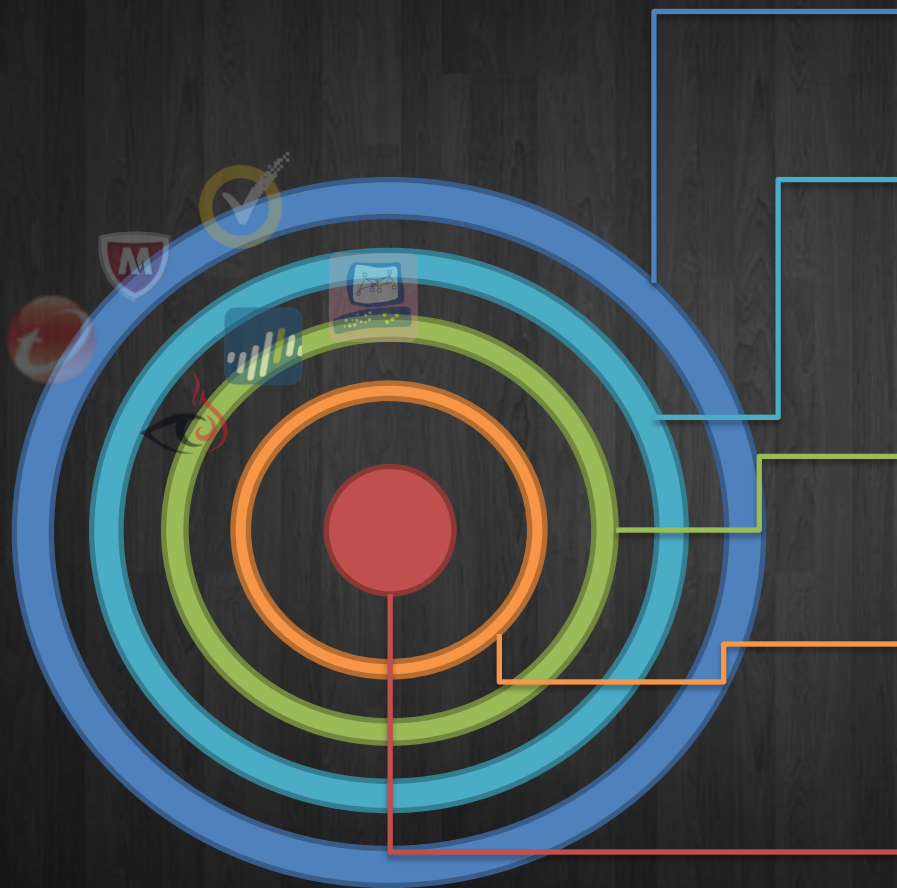
Threats annually



WHY SO MANY ARE UNDETECTED?



Evasion Techniques!



Packers

Designed to turn known code into a new binary

Variations

Slightly alter code to make known code appear new/different

Anti-VM

Designed to make sure code runs only on a real machine

Targeting

Designed to allow code run only on a specific target machine/configuration

Malicious Code

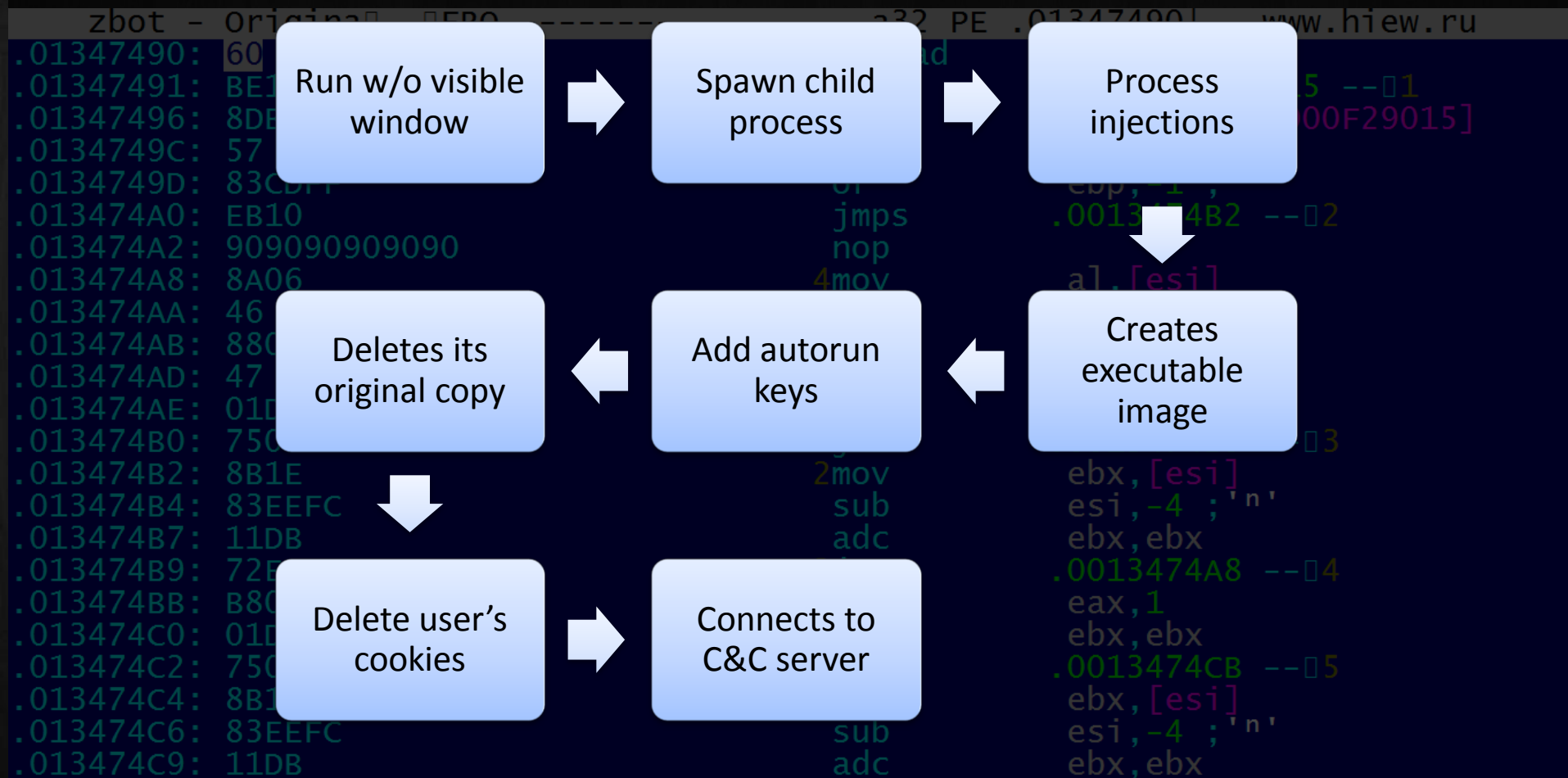
The actual code that runs.
Always the same goals - uses the same techniques

Demo #1

AV vs. Packed Malware



ZBOT: STATIC vs. BEHAVIORS

SHA256: ca1baea714db23b05c0acba0cdbe2ec217e31b95c16519bfd8ac5cc55f994b87



EVERYTHING STARTS WITH (BIG) DATA

DATA COLLECTOR

[ +  +  + REVERSING LABS]

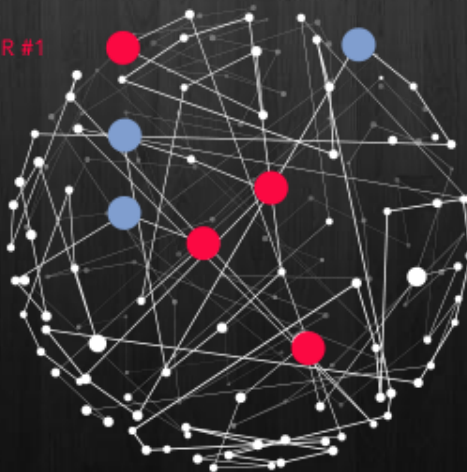


OBSERVER



BEHAVIOR DISTILLER

BEHAVIOR #1



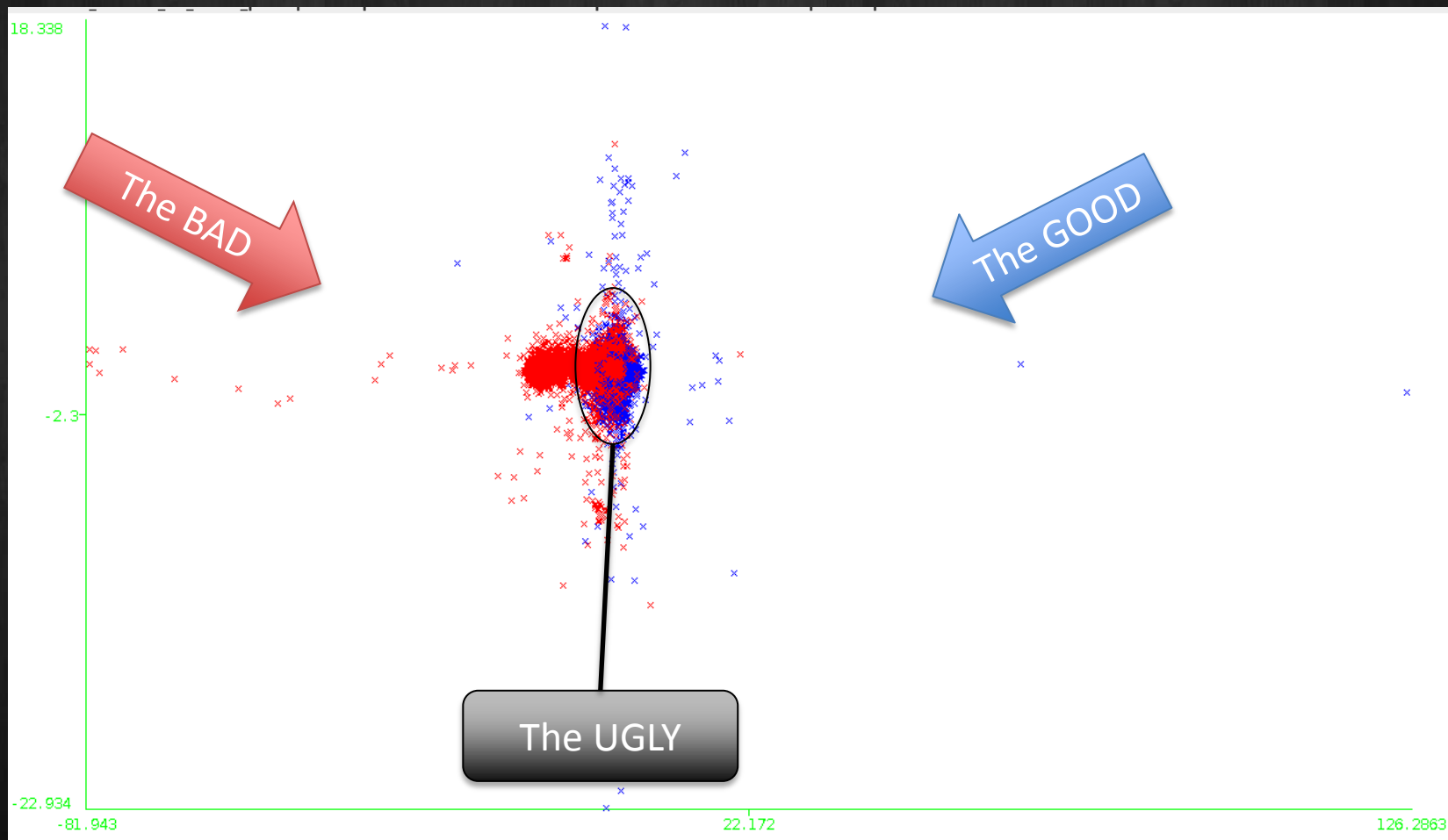
BEHAVIOR #2

BEHAVIOR #3

BEHAVIOR #4

RISE OF THE MACHINE (LEARNING)

- Real data as it looks in the eyes of our algorithms
- BLUE dot represent a benign behavior, RED is malicious

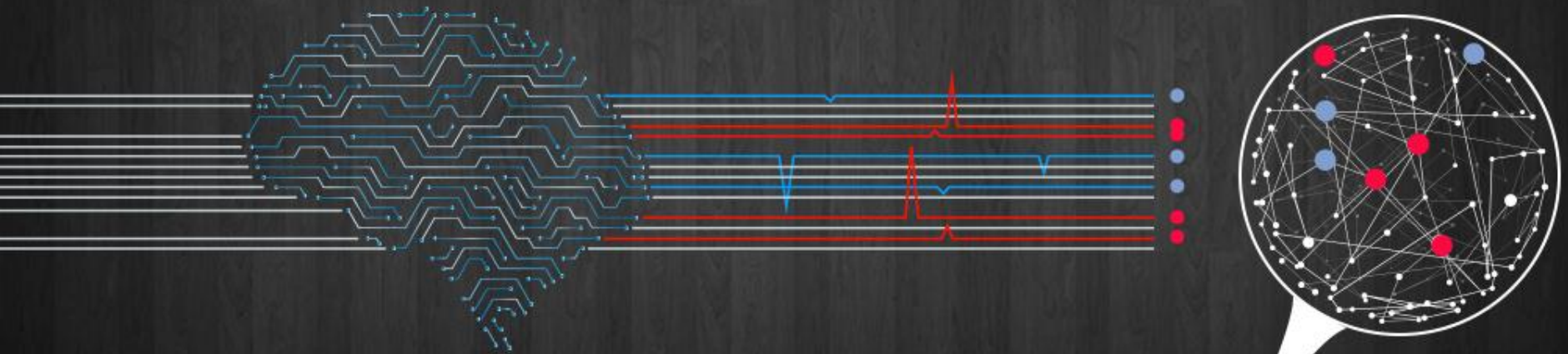


BIG DATA GONE SMALL - OUR AGENT IN ACTION

OS EVENTS



OPERATING SYSTEM FULL CONTEXT VIEW

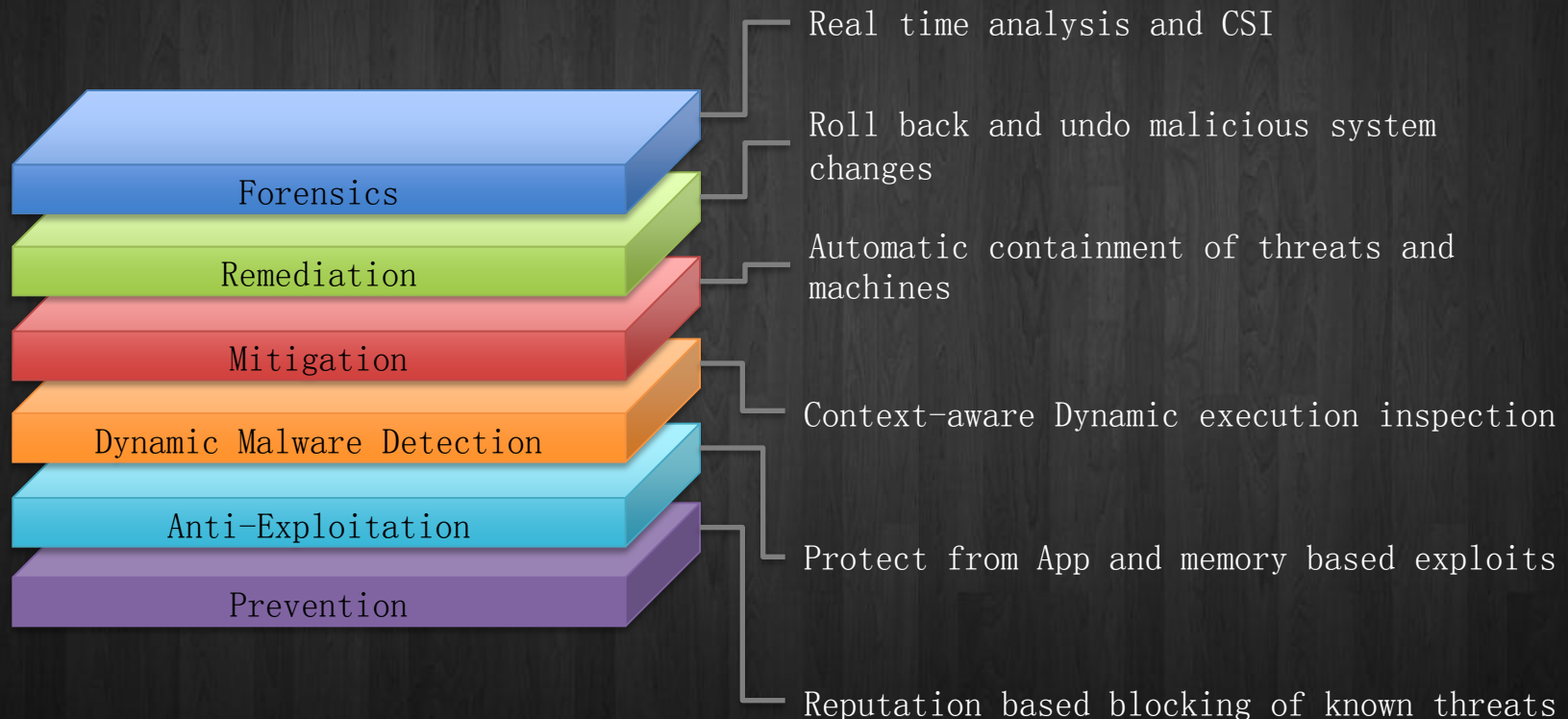


Demo #2

SentinelOne EPP

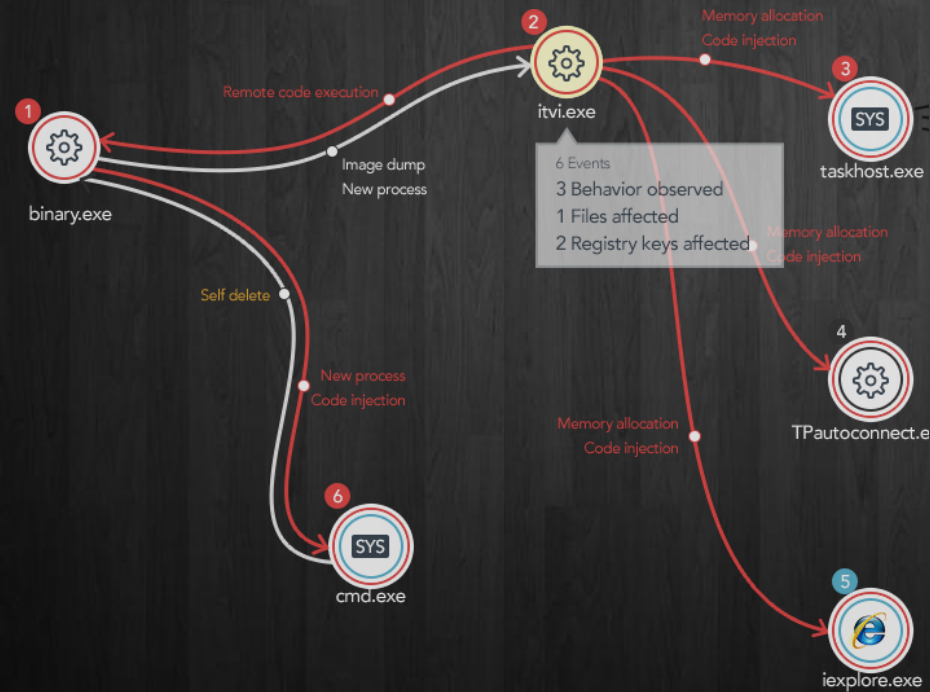
DEFINING NEXT GENERATION ENDPOINT

Six Pillars of NGEP



SentinelOne EPP – The Future is Now

- True Context-aware behavioral detection
- Real-time forensics with visualization
- Cross platform and lightweight



Thank You!

Visit us online for more info:

www.SentinelOne.com

