TrustedSec
INFORMATION SECURITY MADE SIMPLE

BDS
BINARY DEFENSE
IOIOIO SYSTEMS IOIOIO

INFOSEC Today

David Kennedy
Founder, TrustedSec and Binary Defense
@HackingDave, @TrustedSec, @Binary_Defense

David Kennedy's Background

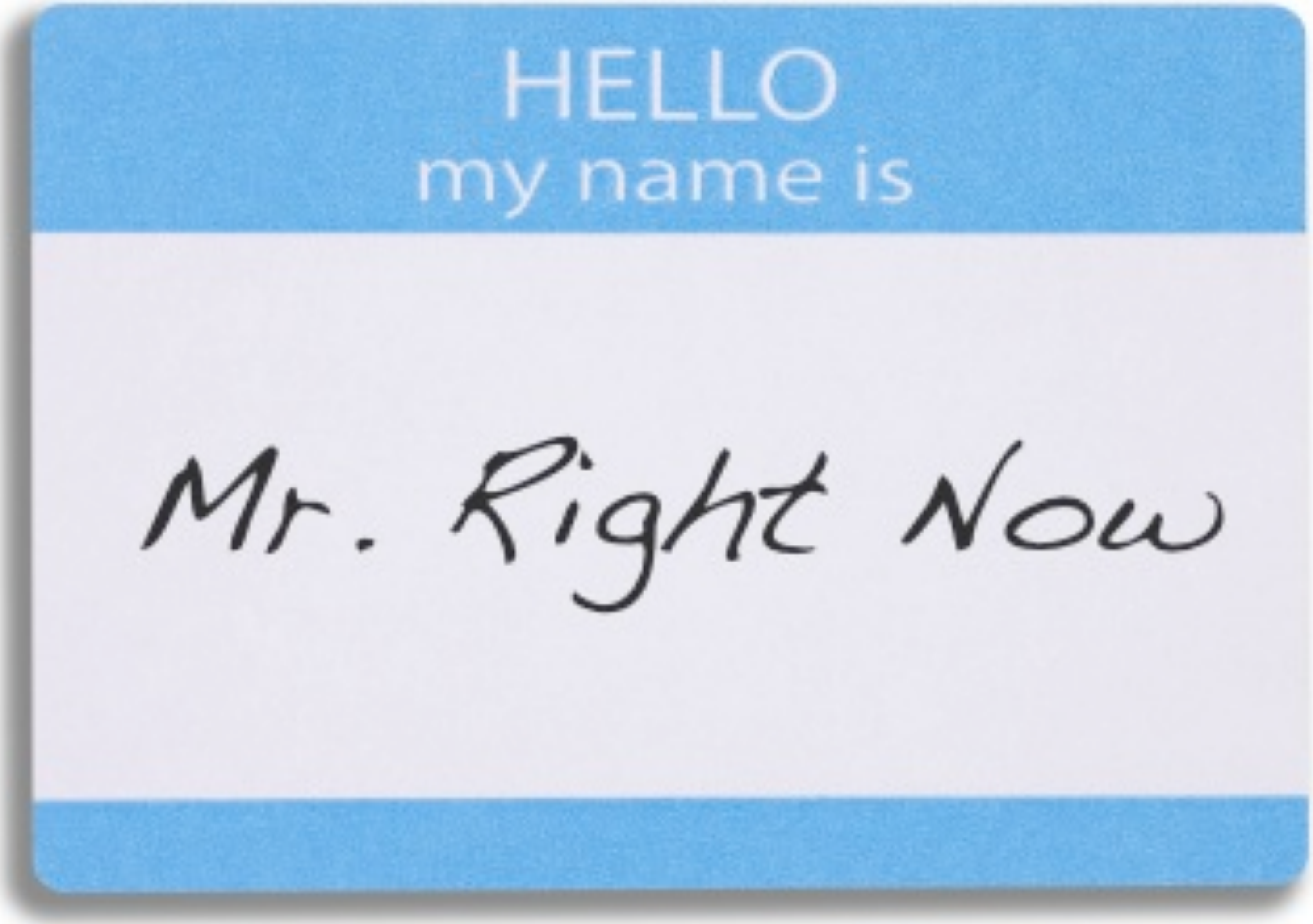
DERBYCON

UNITED STATES MARINE CORPS

IRS HACKING
IRS ESTIMATES IT PAID OUT $5.8 BIL IN FRAUDULENT TAX REFUNDS TO IDENTITY THIEVES IN 2013
ALERT ALER
FOX NEWS LIVE
RPT: MORE THAN 300,000 TAXPAYER ACCOUNTS POTENTIALLY AFFECTED BY CYBERATTACK
A WOMAN, MAN AND TEENAGER OUTSIDE OF TWO
DOW TRN 60.32

TRUSTEDSEC
INFORMATION SECURITY MADE SIMPLE

BDS
BINARY DEFENSE SYSTEMS


HELLO
my name is
Mr. Right Now

Hacking Popularity

Easy Hacking

Explaining 99% of breaches

End-Users

Establish teams

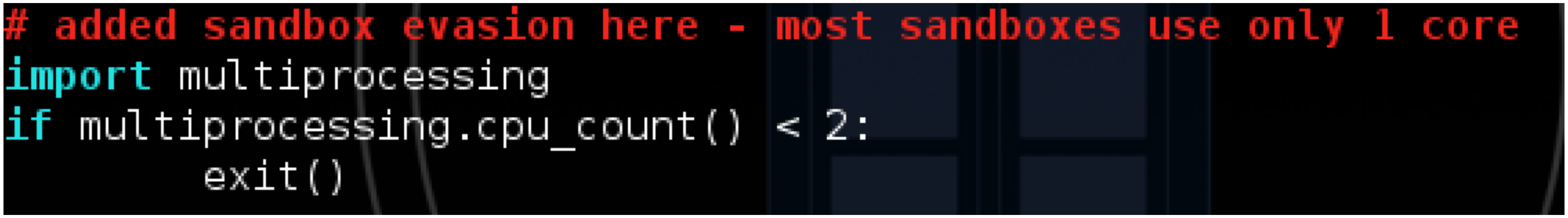
Castle and Archers

SAMSUNG
T··Mobile·
htc
BlackBerry
MOTOROLA
verizon
LG
MESSAGING
NOKIA
at&t
Messaging
12:45
London
Sprint
KYOCERA

TALENT?

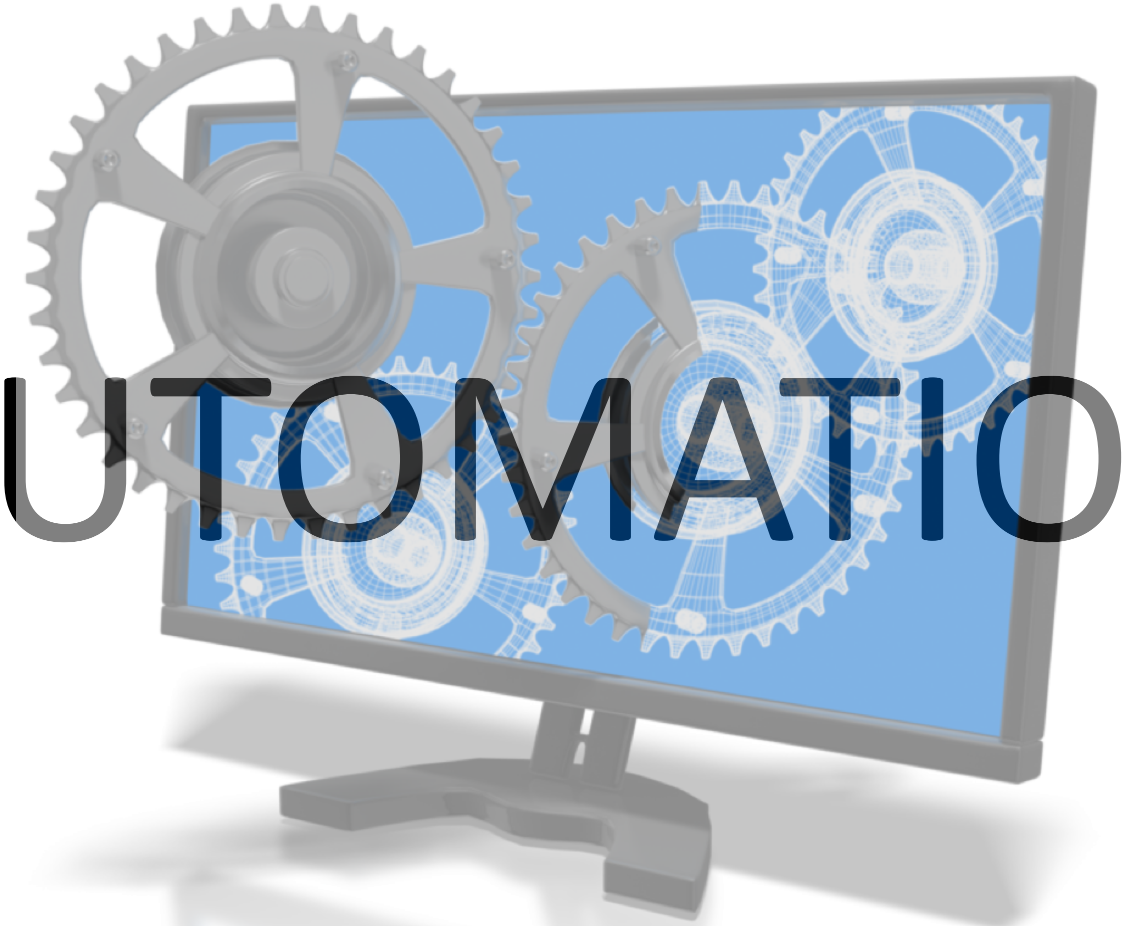
Enter
!
1
@
2
#
3
Q
W
E
A
S
D
Z
X
C
<
>
?

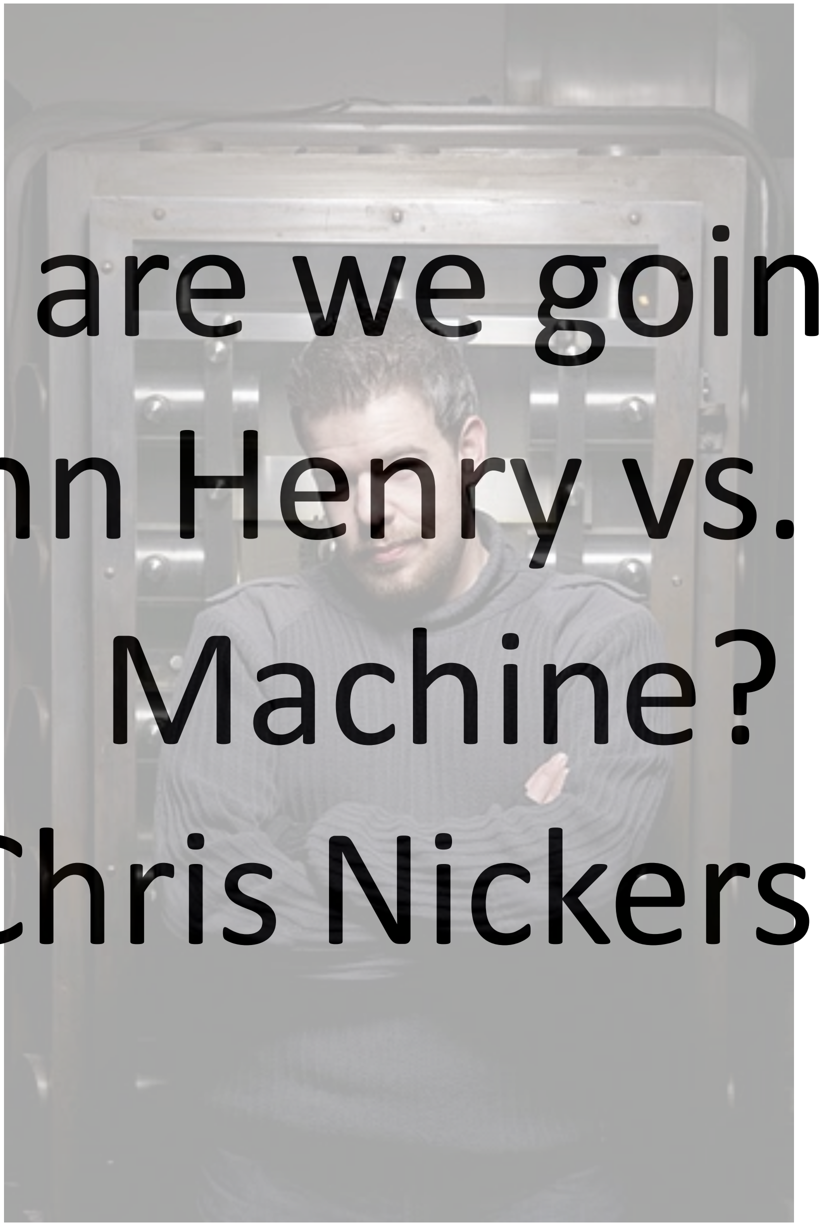
Technology over Talent



```
# added sandbox evasion here - most sandboxes use only 1 core
import multiprocessing
if multiprocessing.cpu_count() < 2:
        exit()
```

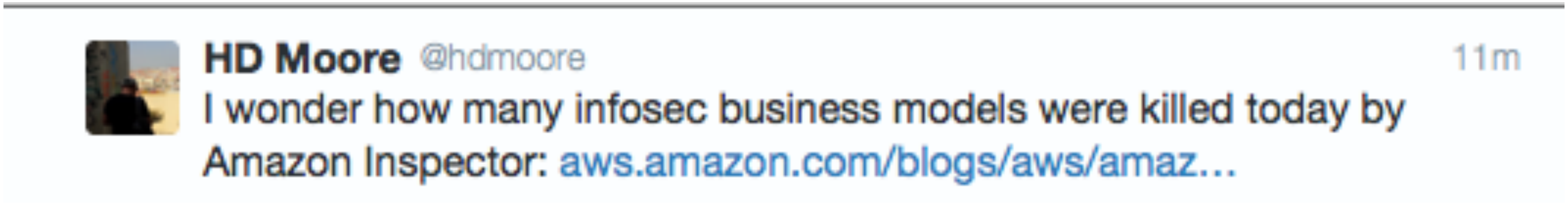
AUTOMATION





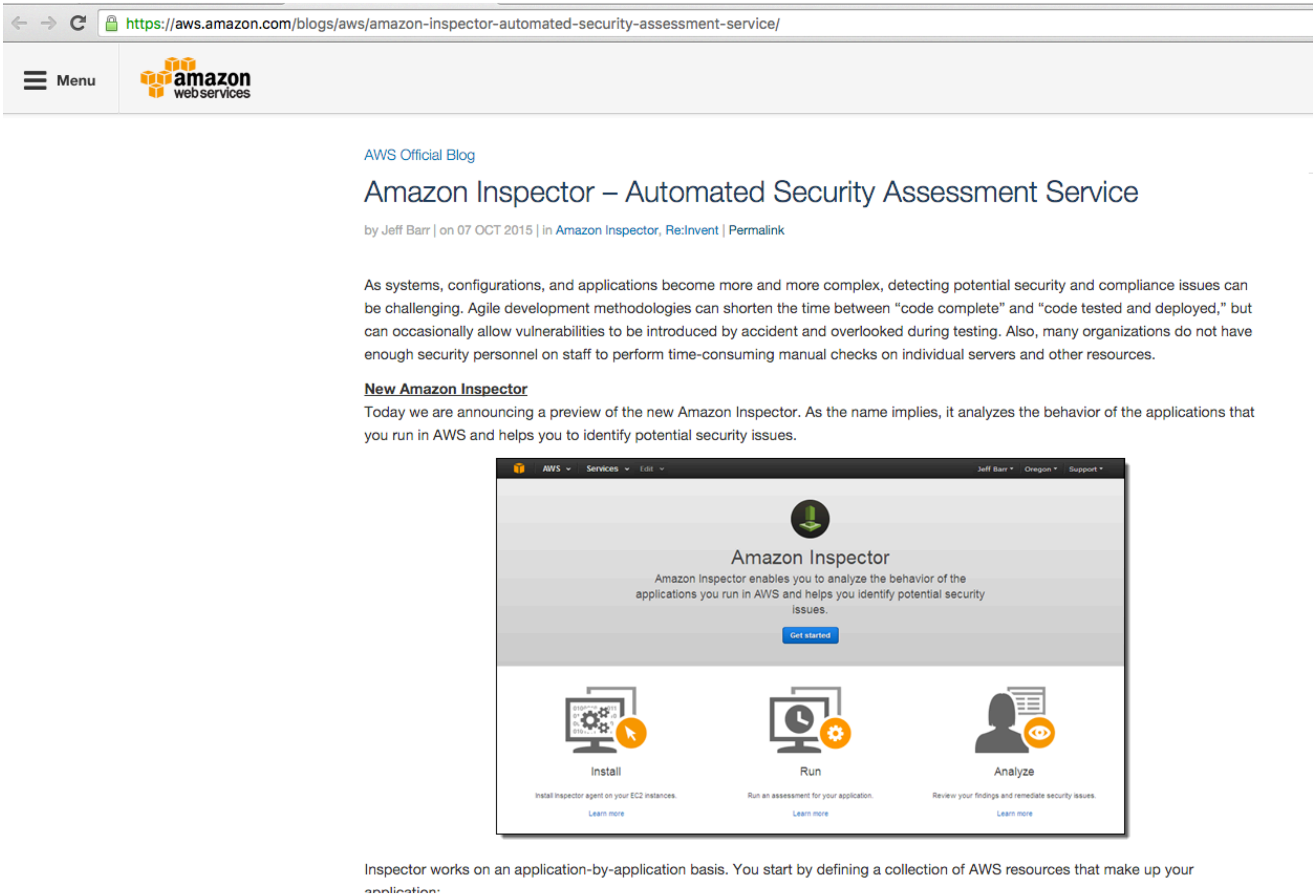
When are we going to be John Henry vs. the Machine?

-Chris Nickerson



HD Moore @hdmoore 11m

I wonder how many infosec business models were killed today by Amazon Inspector: aws.amazon.com/blogs/aws/amaz…


https://aws.amazon.com/blogs/aws/amazon-inspector-automated-security-assessment-service/
Menu
amazon web services

AWS Official Blog

Amazon Inspector – Automated Security Assessment Service

by Jeff Barr | on 07 OCT 2015 | in Amazon Inspector, Re:Invent | Permalink

As systems, configurations, and applications become more and more complex, detecting potential security and compliance issues can be challenging. Agile development methodologies can shorten the time between "code complete" and "code tested and deployed," but can occasionally allow vulnerabilities to be introduced by accident and overlooked during testing. Also, many organizations do not have enough security personnel on staff to perform time-consuming manual checks on individual servers and other resources.

New Amazon Inspector

Today we are announcing a preview of the new Amazon Inspector. As the name implies, it analyzes the behavior of the applications that you run in AWS and helps you to identify potential security issues.

Amazon Inspector

Amazon Inspector enables you to analyze the behavior of the applications you run in AWS and helps you identify potential security issues.

Install

Install Inspector agent on your EC2 instances.

Run

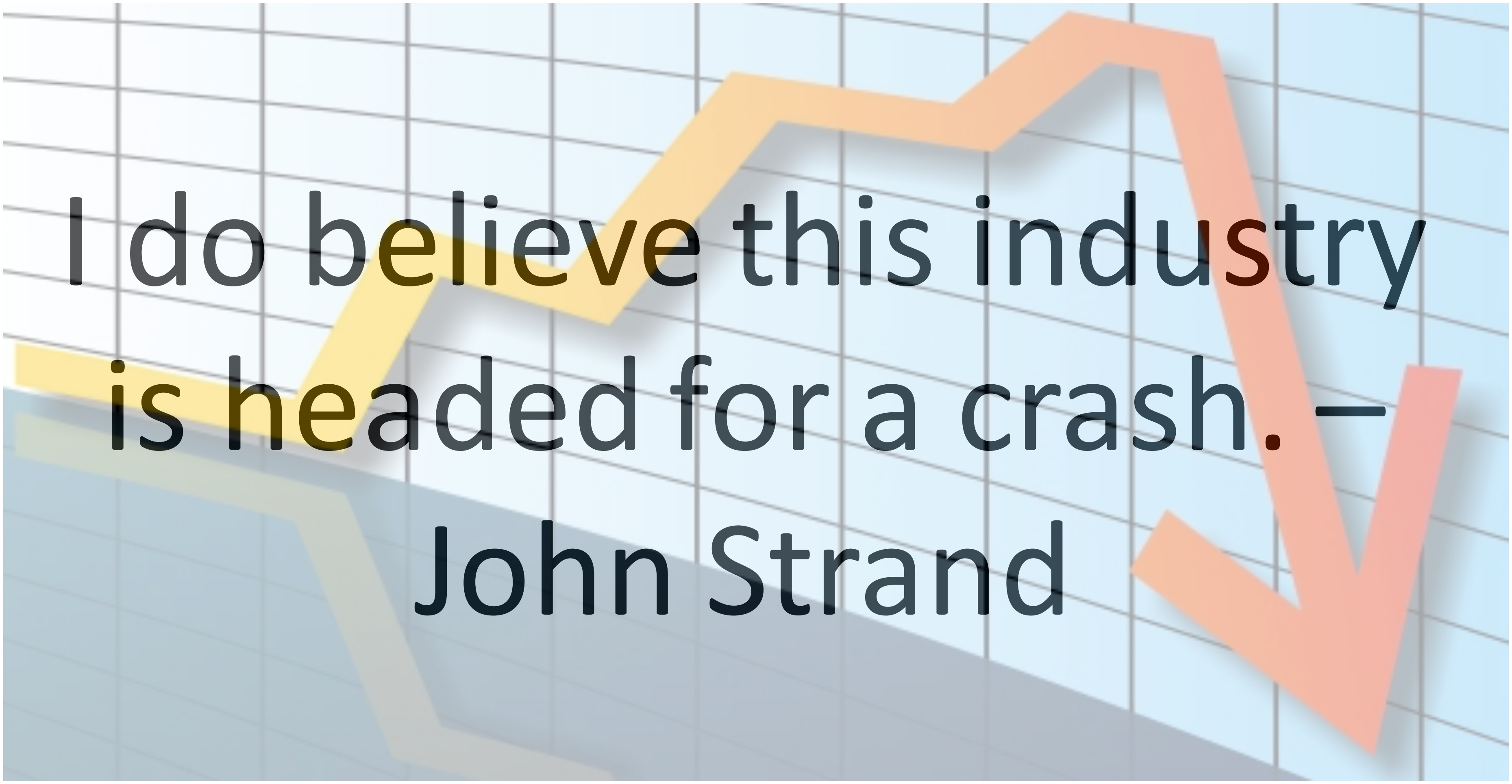
Run an assessment for your application.

Analyze

Review your findings and remediate security issues.

Inspector works on an application-by-application basis. You start by defining a collection of AWS resources that make up your application:

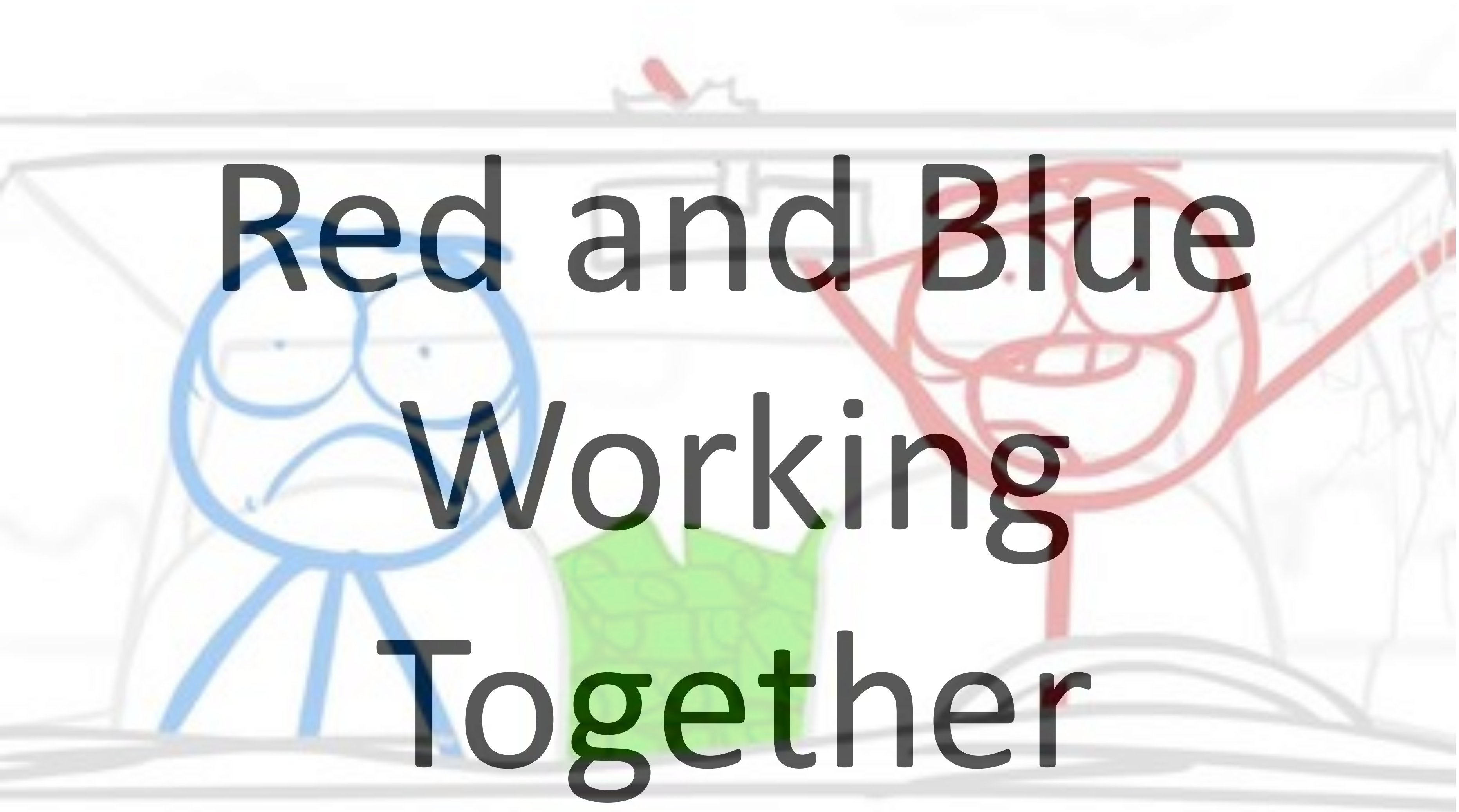
PUPPY MILLS



I do believe this industry is headed for a crash. – John Strand

PCI
DSS
COMPLIANT

Action
Changes
Things



Red and Blue Working Together

SKILLS

Standardize

Good Ideas - Defense

- Disabling local administrator accounts, or randomizing.
- Rotating domain admin account passwords.
- EMET deployed to systems on perimeter and endpoints.
- AppLocker to disallow PowerShell execution for normal users.
- Disallowing executables to be run through TEMP and other directories.
- Network segmentation of user workstations.
- Focus on detection capabilities over anything.
- Removing basic attack vectors just defaults.

BETTER
WORSE

THANK
YOU!