CYLANCE™
CONSULTING

DON'T RESPOND. CONTAIN.

COREY WHITE | SVP, WORLDWIDE CONSULTING
SIG MURPHY | CONSULTING DIRECTOR – WEST NORTH AMERICA

SAFE HARBOR

The information in this presentation is confidential and proprietary to Cylance® and may not be disclosed without the permission of Cylance. This presentation is not subject to your license agreement or any other service or subscription agreement with Cylance. Cylance has no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein.

This document, or any related presentation and Cylance's strategy and possible future development, product, and/or platform direction and functionality are all subject to change and may be changed by Cylance at any time for any reason without notice. The information on this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. This document is for informational purposes and may not be incorporated into a contract. Cylance assumes no responsibility for errors or omissions in this document.

PRESENTERS

COREY WHITE

SVP, Worldwide Consulting,
ThreatZERO, and Education

- 20+ year security career
- Leads the Cylance Consulting team, experts in incident containment, security assessments, and education
- Formerly at Foundstone and McAfee/Intel

SIG MURPHY

Consulting Director – Western North America

- Formerly at Fidelis and the DoD Cybercrime Center (DC3; IA and CI)
- Husband, Father, Gamer (time allowing)

AGENDA

The current state of incident response services

A case study of a real world attack

Why the contain and prevent approach is the future

CURRENT STATE OF INCIDENT RESPONSE SERVICES

- How many **repeated ransomware incidents** have you had?
- How many **multiple variants of same malware** have you had to deal with over the years?
- How many incidents have you done forensics and found out **data was exfiltrated months before you detected it**?

Average hack takes 197 days to be detected

[1] *Source: Ponemon Institute | 2018 Cost of a Data Breach Study*

CURRENT THREAT LANDSCAPE

The percentage of hosts we install on that have **malware that previously went undetected…and un-prevented**.

The percentage of **spear-phishing that is now ransomware,** up almost 800% since previous quarter (PhishMe).

The percentage of breaches that had a **financial or espionage motive**.

The percentage of **malware that can be stopped with AI.**

INCIDENT RESPONSE VICIOUS CYCLE

IT teams spend hours re-building or re-imaging of machine

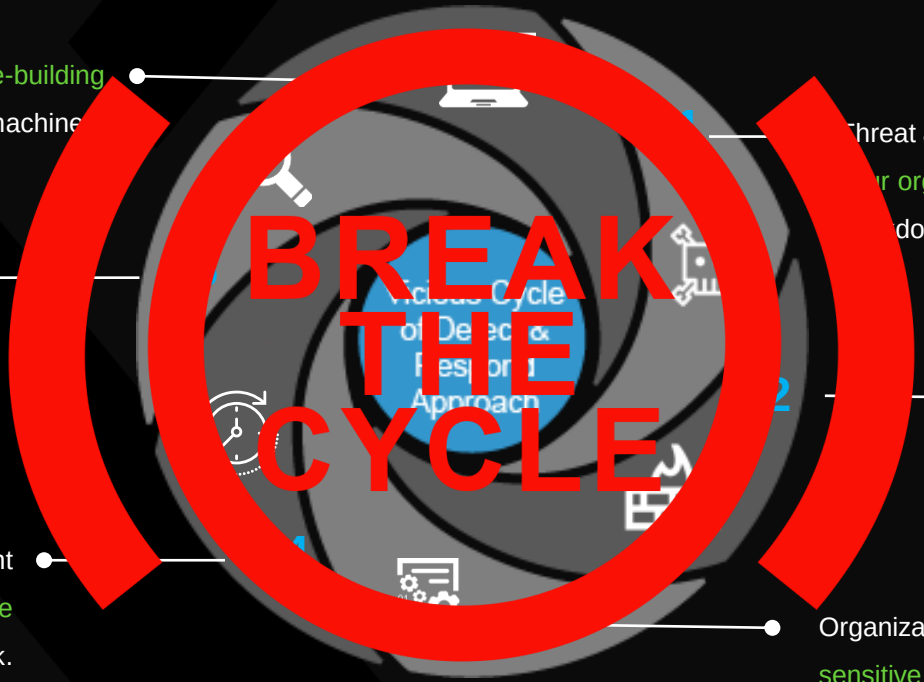
Threat actors gain access to r organization via malware, door, and other exploits.

Threat actors use backdoor to evade the investigation and gain persistent access.

Sophisticated attacks bypass or evade existing security controls.

Hours and weeks are spent in investigating the cause of the attack.

Organizations lose sensitive corporate data or become victims of ransomware.



COSTS FOR COMPROMISED ENDPOINTS

Source: 451 Research 2018

$6

TRILLION

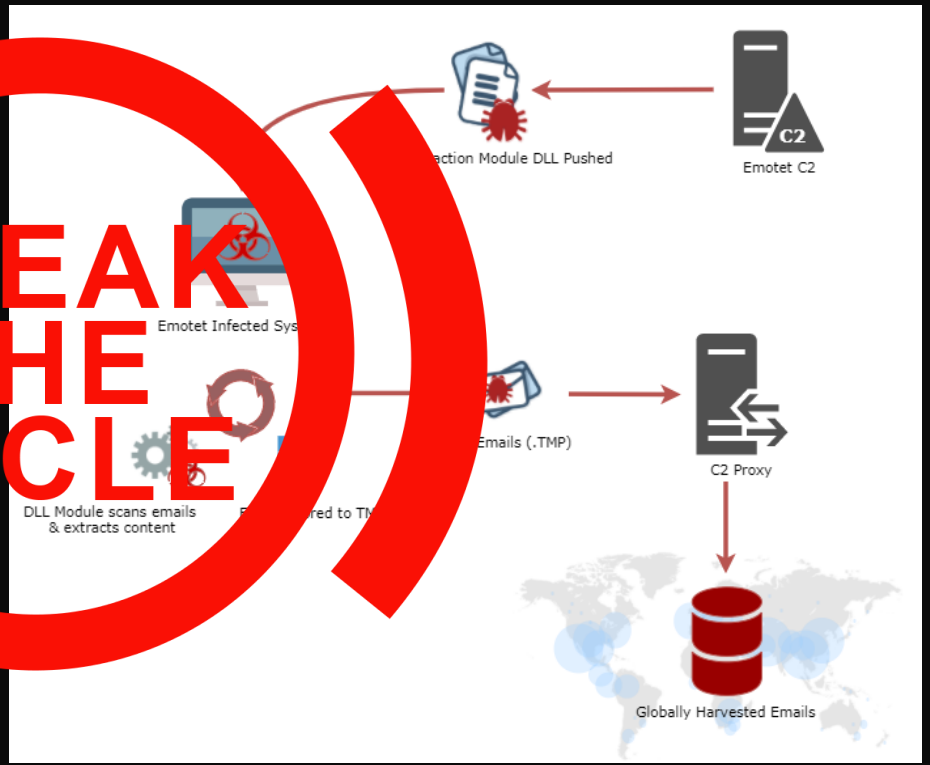
Estimated annual cybercrime damage by 2021. To put that in perspective, that's almost 10 percent of the world economy.

U.S. Department of Homeland Security

EMOTET CASE STUDY

- Hundreds of versions of e 201
- We have done 100+ in nts on-Cylance customers
- Aggressive spread
- Constant re-infectio
- "The most costly and truct malware affecting sta cal, t l, and territorial (SLTT) gover ts, a e private and public sectors," – costing governments up to $1M per incident[1]

Source: US-CERT Alert (TA18-201A)



THE EVOLUTION TO PREVENTION

LEGACY

- One of the tools detects “something”
- Reactive
- Image the entire disk and/or memory
  - Time consuming
  - Large amount of data
- Requires hardware/appliances in environment for additional visibility
- Increase in capital costs
- “Seize all, find all”

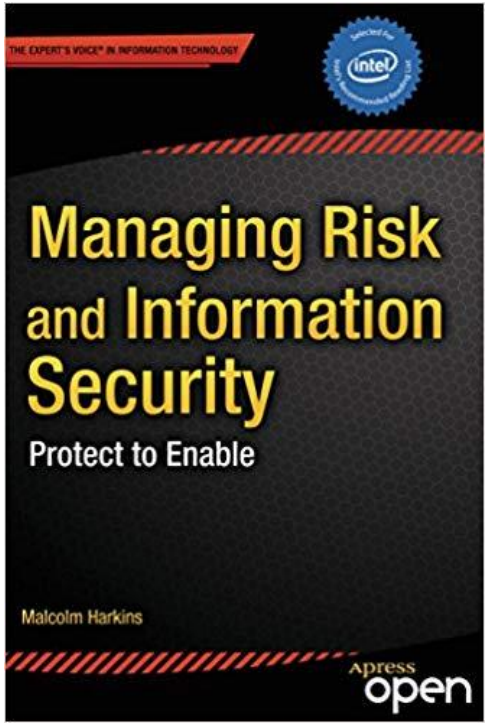
PREVENTION-BASED INCIDENT CONTAINMENT

- No network taps or monitoring of egress points
- Assesses every endpoint
- Leverage your software deployment to push out dissolvable scripts and/or through the agent
- Principle of least data
- Speed in analysis – we’re TWICE as fast!
- Use AI for detection of malware, PUPs and compromised credentials
- Containment with a single mouse click

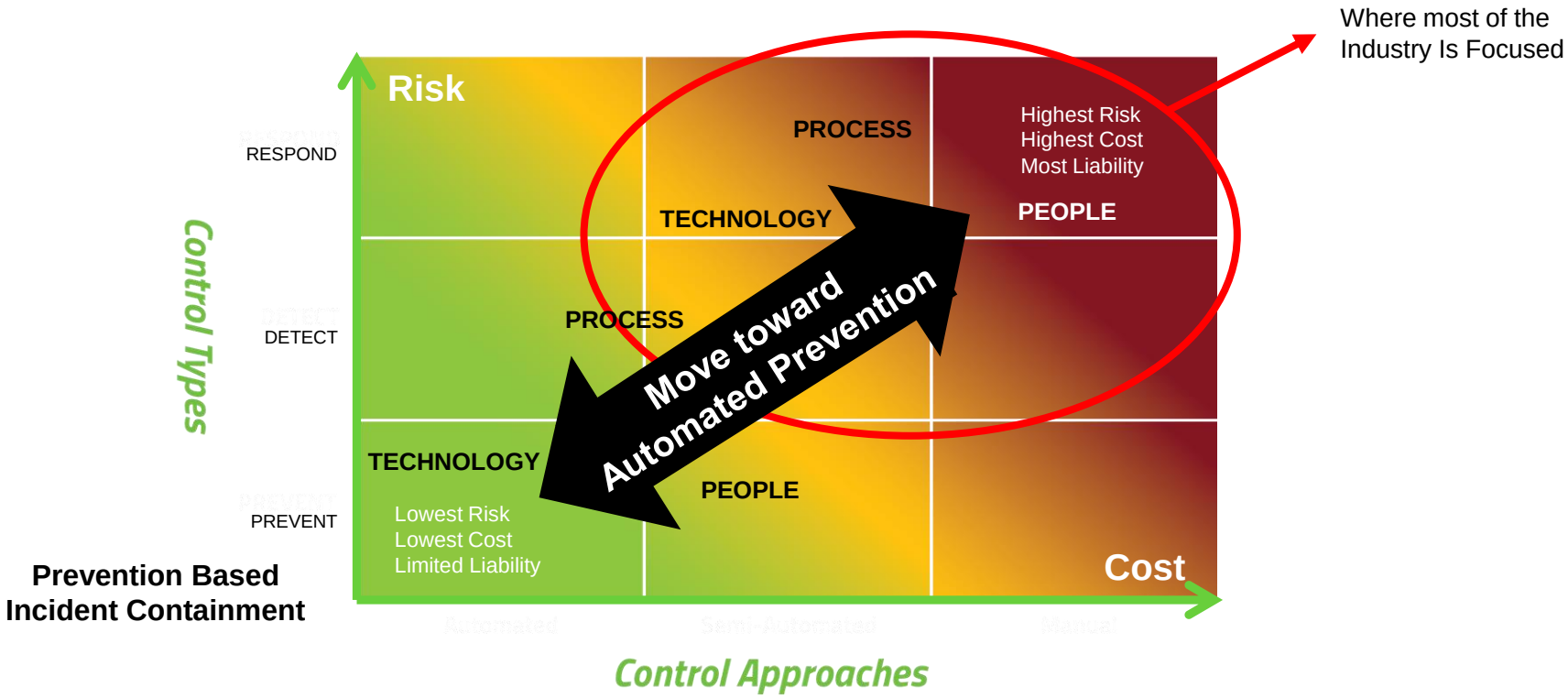
Oxymoron?

MANAGING RISK

- Author Malcolm Harkins
- Describes changing risk environment and why a fresh approach is needed
- Discusses business risk from a broader perspective



GETTING TO AUTOMATED & MANAGED PREVENTION



WHAT DOES PREVENTION LOOK LIKE?

- How do you quantify prevention?
- How do you know your compromise has been contained?
- How do you know there is NOT more malware out there?

CYLANCE

Report Card

Grading Scale:

95 – 100% - A
94 – 85% - B
84 and Less - C

Files Analyzed	787,688,185
A	Overall Grade: 95.94%

Coverage Breakdown:

*Report generated as of 08/16/2016

Category	# Of Hosts/Files Under Category	Percentage Of Category	Description
Malware	7,022/7,098	98.92%	*The number of malware threats that have been quarantined.*
Potentially Unwanted Programs (PUPs)	33,745/34,259	98.50%	*The number of PUPs that have been quarantined/removed or whitelisted.*
Auto-Quarantine	13,355/13,452	99.28%	*The number of devices with Auto-Quarantine enabled for Unsafe and Abnormal threats.*
Memory Protection	13,060/13,452	97.08%	*The number of devices using Memory Protection in Block or Terminate mode.*
Script Control	12,904/13,452	95.93%	*The number of devices using Script Control in Block mode.*
Asset Inventory	11,679/13,452	86.82%	*The number of devices that have been online in the last 30 days.*
Upgrade Management	12,783/13,452	95.03%	*The number of devices on either of the two most recent versions of CylancePROTECT.*

GLOBAL INCIDENT CONTAINMENT COVERAGE

Follow-the-sun, non-stop incident containment capabilities

YOUR PARTNER IN PREVENTION

- We are **evolving the industry** from incident response and monitoring to incident containment and prevention
- Our practice is based upon **making a difference for your company FIRST**
- Our goal is not to profit from your incident – **we succeed together** based upon a preventative approach

QUESTIONS

AND

ANSWERS

Get to Containment

Contact us for your Incident Containment Readiness Assessment and free 1-hour consultation with one of our prevention experts.

proservices@cylance.com
+1-877-973-3336

Learn more about our Incident Response and Containment service:
rebrand.ly/contain