Data Security Solutions (DSS)

Tim Seppi – Dell Security Specialist

March 30, 2017 **MEEC Conference**

Why Security at Dell?

"Security has got to be part of what you do every single day. Across the entire spectrum, **we are embedding security in everything that we do**..."

– Michael Dell

Cyber Security Best Practices: +95% of attacks at the endpoint

1. Cyber security awareness campaign
2. Vulnerabilities: Inventory and patch management:
3. Multi factor authentication
4. Protect data with encryption
5. Predict and prevent malware attacks
    5. An ounce of prevention is worth a pound of cure i.e. EDR

Why Your Antivirus Isn't Working Anymore.

Tim Seppi | Data Security Solutions
Andreas Xenos | Engineer

Symantec's senior vice president Brian Dye declared to the Wall Street Journal that antivirus "is dead.. May 2014

Trend Micro’s CEO, Eva Chen, threw down the gauntlet to her competitors last week, proclaiming that hackers are ahead of the game and that the anti-virus industry “sucks” Jun 2008

CYLANCE™

2016 VERIZON DBIR

- Malware is used in 90% of cyber incidents
- Adversaries create huge numbers of malware variants to avoid detection… or they design one just for you
- Unique malware is the norm rendering traditional AV totally useless.

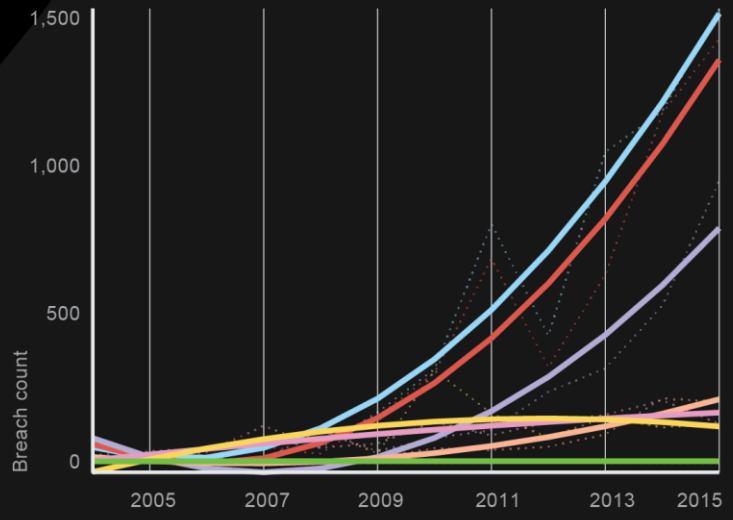


Figure 1.

Number of breaches per threat action category over time, (n=9,009)

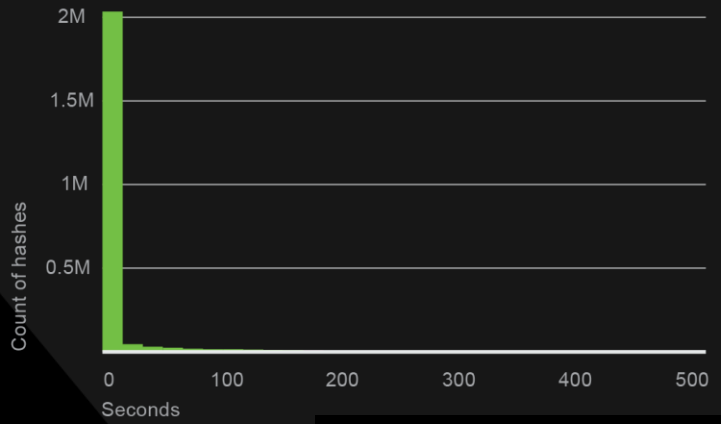


Figure 2.

Count of hashes by lifespan in seconds, (n=2.3 million)

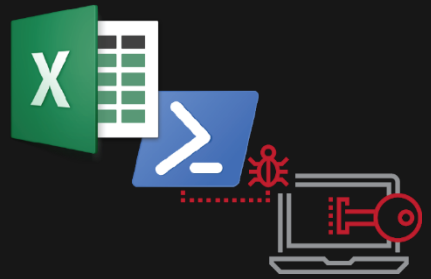
Source: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

CYLANCE™

COMMON VECTORS OF ATTACK

EMAILED DOC WITH MALICIOUS MACRO FETCHES MALWARE

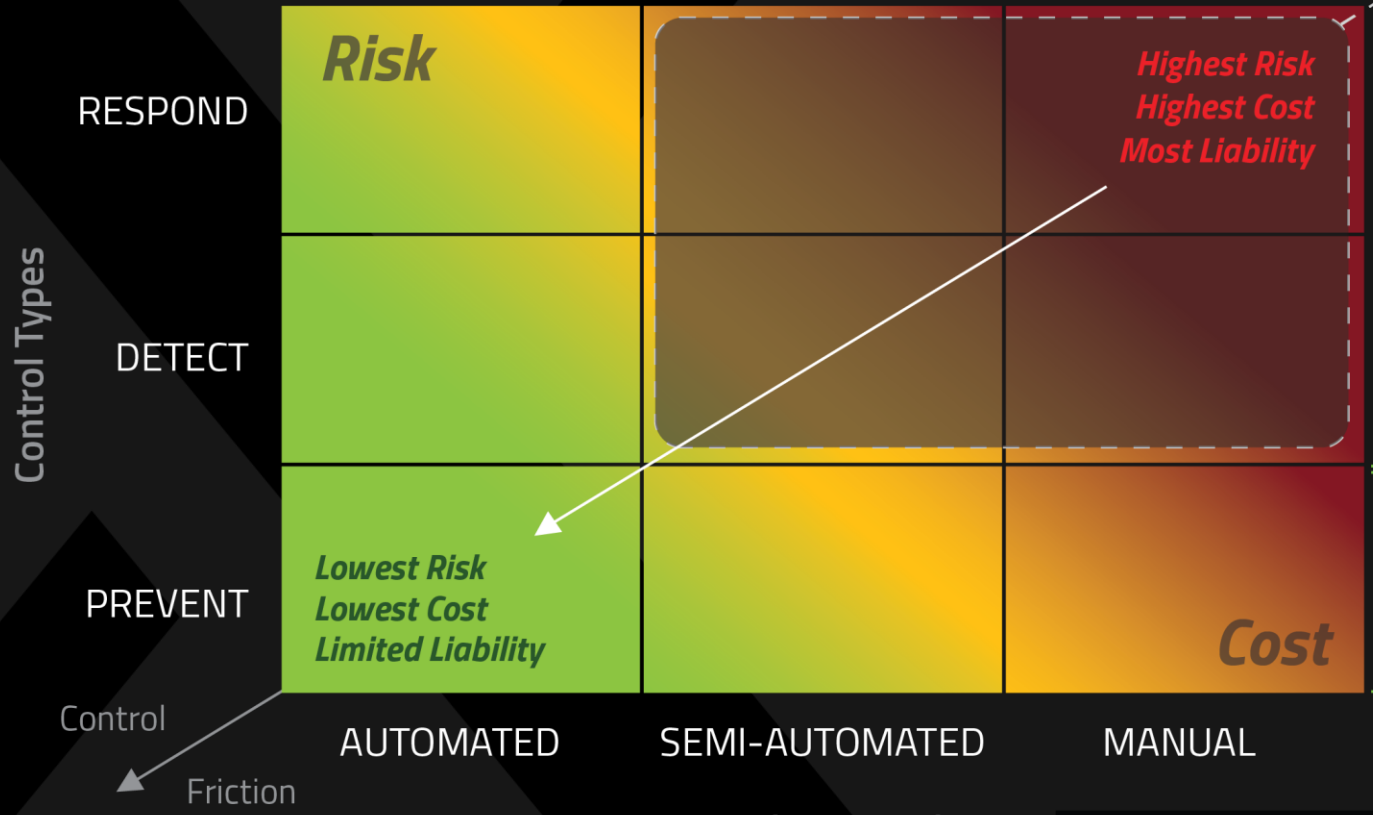
USER DOWNLOADS MALWARE



DOC WITH MALICIOUS POWERSHELL FETCHES CODE TO DUMP CREDENTIALS

CYLANCE™

Risk Mitigation Cost



Where most of the industry is focused

Focus is on minimizing damage – only variables are time to detect and time to contain

Focus is on minimizing vulnerability and potential for harm

CYLANCE

Source: Managing Risk and Information Security 2nd Edition Malcolm Harkins

Past Present & Future of Security

Past | Present | Future

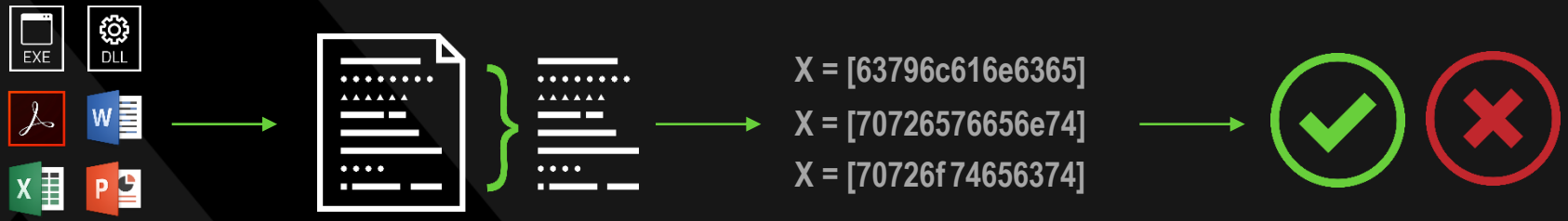
Humans Needed

Specialized Humans Needed
Post-Execution

No Humans
Pre-Execution

HOW IS IT DONE?

ALGORITHMIC SCIENCE AND MACHINE LEARNING



COLLECT

EXTRACT

TRANSFORM, VECTORIZE AND TRAIN

CLASSIFY AND CLUSTER

CYLANCE™

Leverage the power of machines, not humans, to dissect malware's DNA. Artificial intelligence then determines if the code is safe to run.

NEXT GENERATION

RELY ON AI & ML

ANALYZE MALWARE AT THE DNA-LEVEL

ADVANCED THREAT PREVENTION

MINIMAL UPDATES

WORK ON AIR GAPPED NETWORKS

PREDICT AND PREVENT

TRADITIONAL APPROACH

RELY ON HUMAN CLASSIFICATIONS

REQUIRE ON-PREMISE INFRASTRUCTURE

WAIT FOR THREATS TO EXECUTE

REQUIRE CONSTANT UPDATES

SIGNATURES

HEURISTICS

BEHAVIORAL ANALYSIS

MICRO-VIRTUALIZATION

SANDBOXING

CYLANCE™

QUESTIONS AND ANSWERS

CYLANCE™