PSI Tech Expo

Sept 4th, 2014

Protecting your Assets

Presented by:
Chris Nyhuis – Vigilant LLC.

VIGILANT
TECHNOLOGY SOLUTIONS

9/16/14

Know More. Secure More.

Chris Nyhuis

cnyhuis@vigilantnow.com
http://www.vigilantnow.com

- Owner of Vigilant Technology Solutions an IT Cyber Security Personal Training Firm.
- In Security and IT Industry 17 Years
- Cyber Security Instructor at Advanced Technical Intelligence Center (Dayton)
- Madly in love with my family
- Passionate about Orphan Care

Agenda

- Understanding the Problem
- How attacks have changed and the Security industry hasn't
- Lower your exposure and breach costs

Understanding the Problem:
The Compliance and Security Myth

Compliance

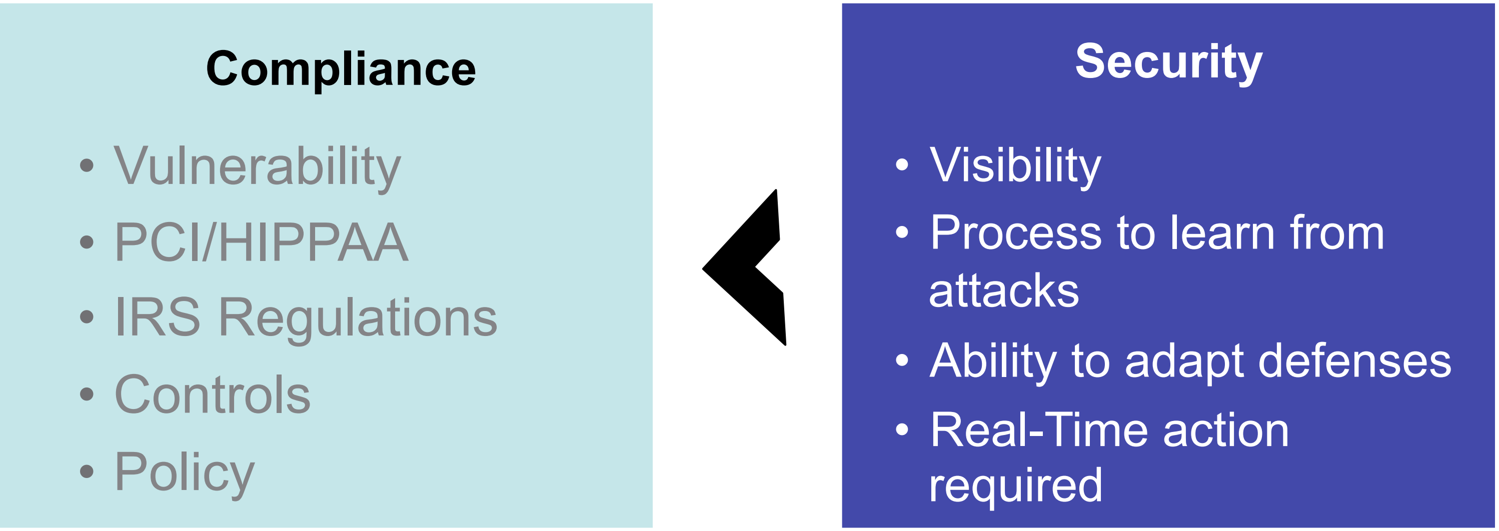
- PCI
- HIPPAA
- IRS Regulations
- Controls
- Policy

≠

Security

- Visibility
- Process to learn from attacks
- Ability to adapt defenses
- Real-Time action required

Understanding the Problem
The Compliance and Security Myth



Compliance

- Vulnerability
- PCI/HIPPAA
- IRS Regulations
- Controls
- Policy

Security

- Visibility
- Process to learn from attacks
- Ability to adapt defenses
- Real-Time action required

What do these companies have in common?

Neiman Marcus

HealthNet

ZAPPOS

Nasdaq

CITIGROUP

EBAY

TARGET

AOL

U.S. Government

What do these companies have in common?

They were all compliant…

HealthNet
1,500,000

Heartland
130,000,000

ZAPPOS
24,000,000

Nasdaq
Not Known Yet

CITIGROUP
3,900,000

EBAY
145,000,000

TARGET
70,000,000

AOL
92,000,000

T.J. MAXX
94,000,000

Ponemon’s Cost of Data Breach Study:
Global Study, sponsored by IBM.

Studied 314 companies spanning 10 countries..

- Average total cost of a Data Breach increased by 15%
- Average of $3.5 million
- Cost per record is $145.00
- Your Reputation is priceless

VIGILANT

TECHNOLOGY SOLUTIONS

WWW.VIGILANTNOW.COM - SALES@VIGILANTNOW.COM

Take Away #1

Security is not the same as Compliance – Security is a balance of Control and Visibility

Understanding the Problem:
The threats have changed

Before

- Random Small Attacks
- Attackers were more randomly skilled
- I'm too small - Big targets were the focus

Today

- Highly designed organized attacks
- Attackers are skilled - APT
- Attacks are coming through supply chain

VIGILANT

TECHNOLOGY SOLUTIONS

WWW.VIGILANTNOW.COM - SALES@VIGILANTNOW.COM

Take Away #2

SMB is the new gateway – Protect your reputation you may be the path

Understanding the Problem: Threat protection has changed

Before

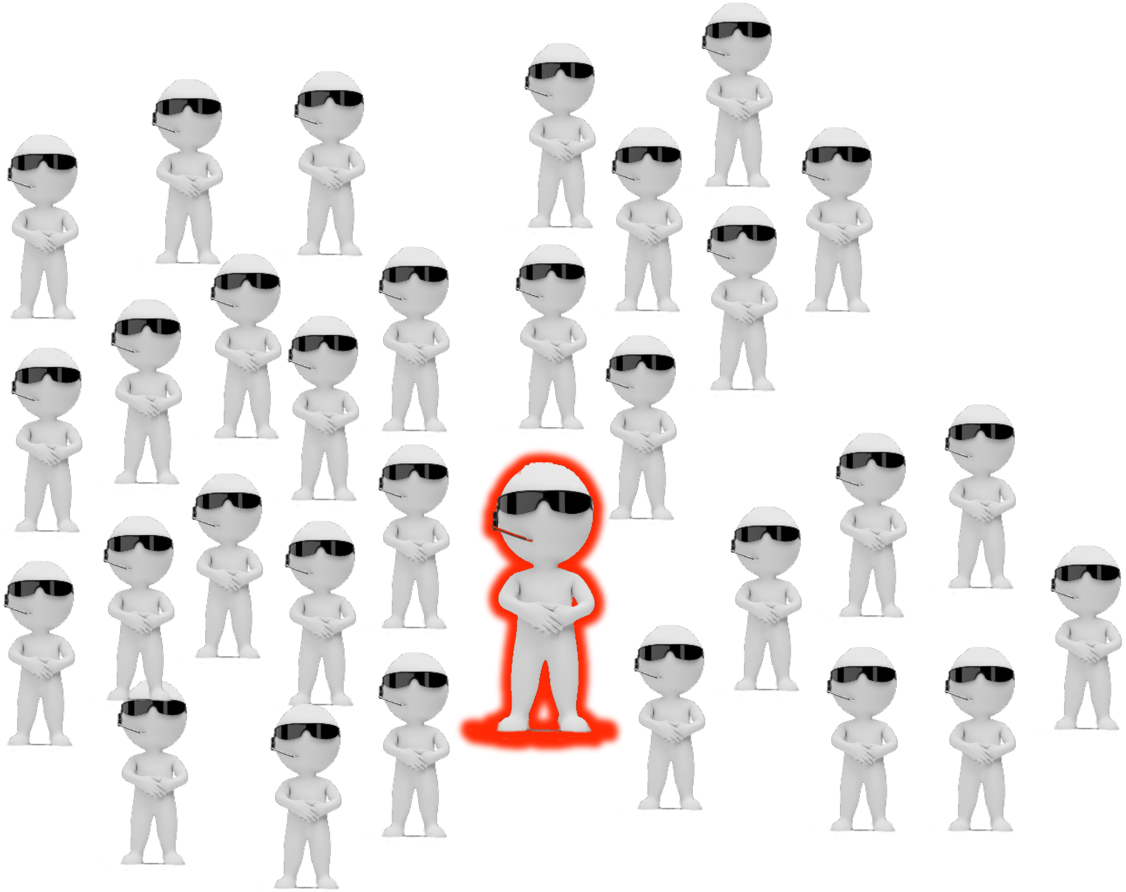
- Signatures - The Herd Mentality Protection

Today

- Attacks are more targeted

That is why…

- 54% of malware typically evades anti-virus detection
- Less than 2% of breaches are detected in the first 24 hours, less than 46% in the first 30 days
- 60% of breaches have data exfiltrated in first 24 hours
- A Trustwave study considered 450 global data breach investigations, as well as thousands of penetration tests and scans. It found that the average time between an initial breach and detection was **210 days**. In 2011 it was 90 Days.
- Over 92% of breaches are discovered by a third party or customer



And if you
are the only
one you may
never know

And because of that…

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

The security industry doesn't like that.

VIGILANT

TECHNOLOGY SOLUTIONS

WWW.VIGILANTNOW.COM - SALES@VIGILANTNOW.COM

Take Away #3

AV is dead, it does not make you safe it is only a layer of protection and not a good one but still useful

Understanding the Problem:
The threat protection has changed

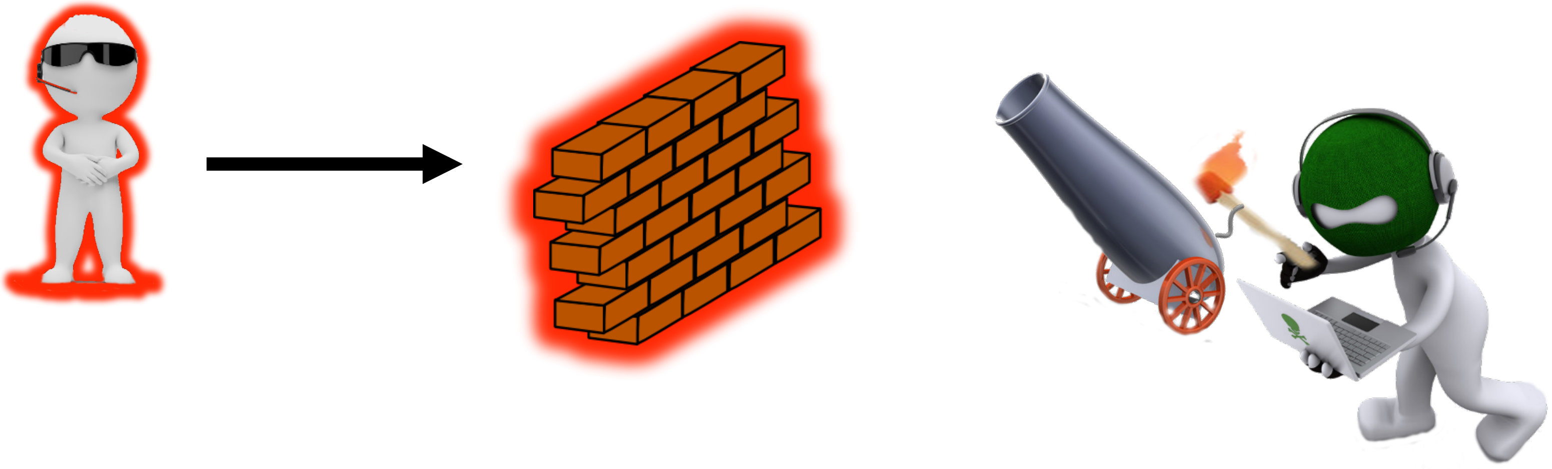
Before

- Signatures - The Herd Mentality Protection
- Automated Alerting
- UTM / Trad Firewalls on perimeter 100% Secure

Today

- Attacks are more targeted
- Combination of Automation and People
- Anomaly Detection - They are in, find them quick

Understanding the Problem: Why UTM Firewalls can’t be your only defense – Signature and Position



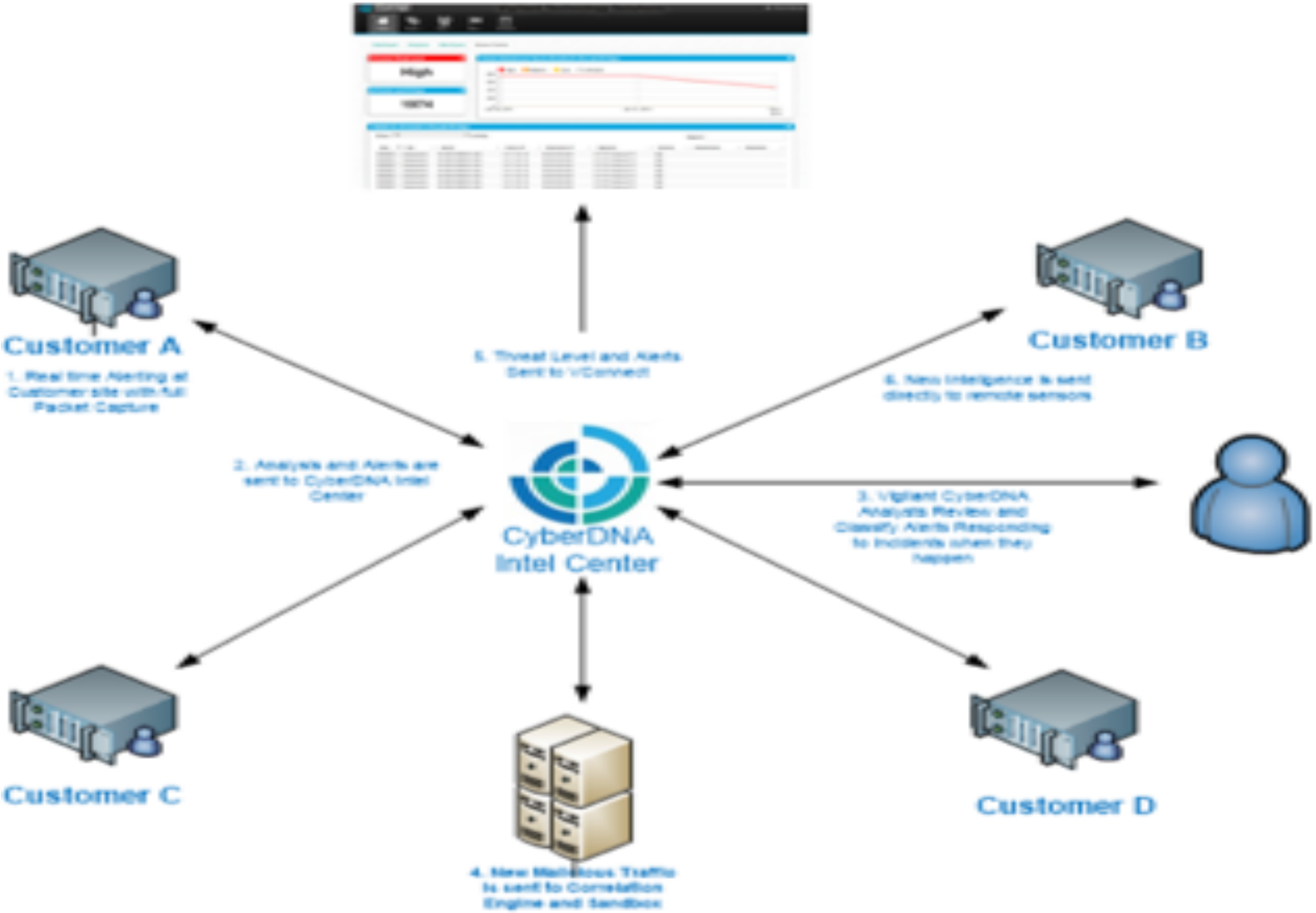
Protecting yourself and lowering your costs:

- Have solid security and high visibility
- Train your team
- Anomaly and Heuristic Intelligence based detection.

CYBERDNA™

VIGILANT
TECHNOLOGY SOLUTIONS

Advanced Network Security Monitoring



Customer A

1. Real time Alerting at Customer site with full Packet Capture

2. Analysis and Alerts are sent to CyberDNA Intel Center

3. Vigilant CyberDNA Analysts Review and Classify Alerts Responding to Incidents when they happen

4. New Malicious Traffic is sent to Correlation Engine and Sandbox

5. Threat Level and Alerts Sent to VConnect

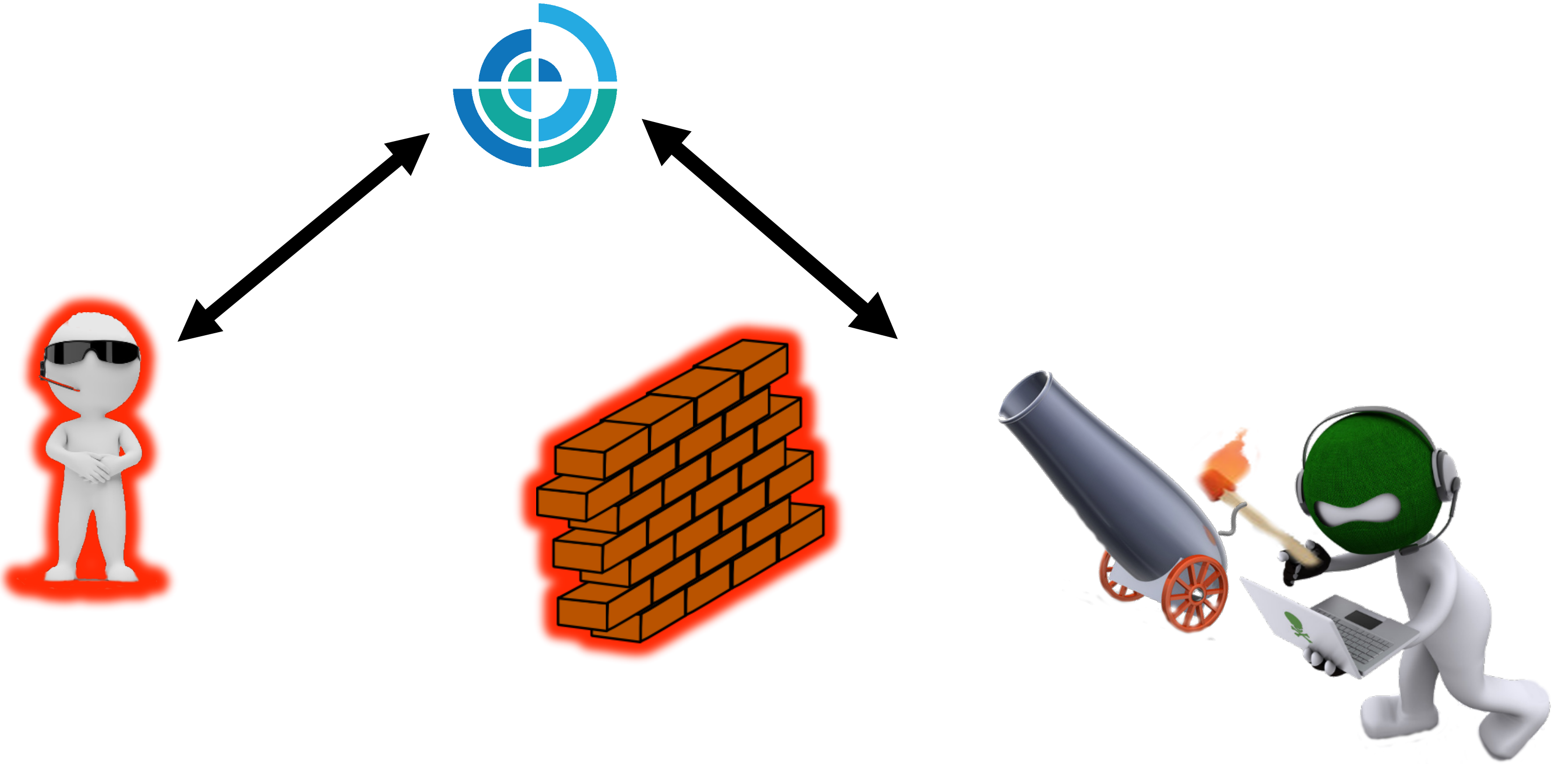
6. New Intelligence is sent directly to remote sensors

Customer B

CyberDNA Intel Center

Customer C

Customer D



VIGILANT

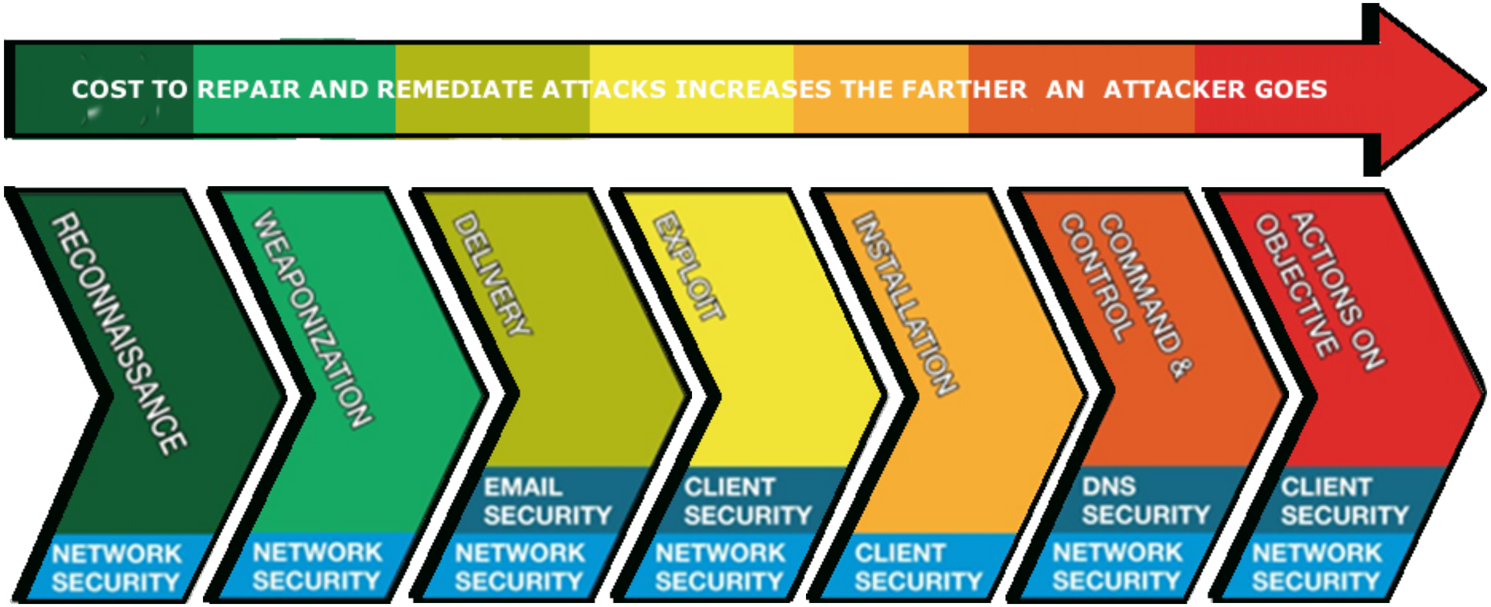
TECHNOLOGY SOLUTIONS

WWW.VIGILANTNOW.COM - SALES@VIGILANTNOW.COM

Take Away #4

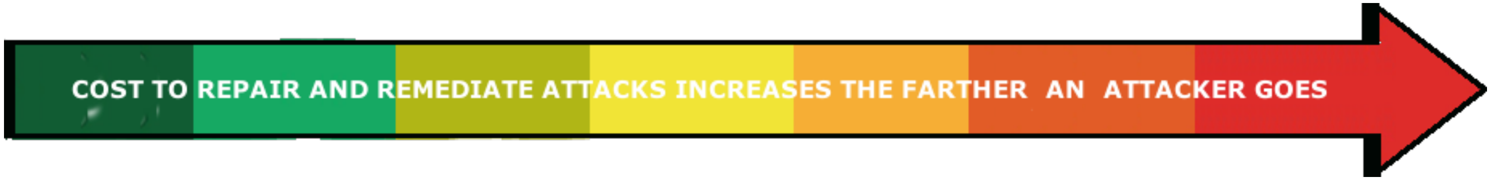
Act like they are already in – Anomaly and Passive detection is imperative

Lower Your Costs - Use tools to Catch them early



Lockheed Martin Kill Chain ®

Lower Your Costs - Use tools to Catch them early


COST TO REPAIR AND REMEDIATE ATTACKS INCREASES THE FARTHER AN ATTACKER GOES

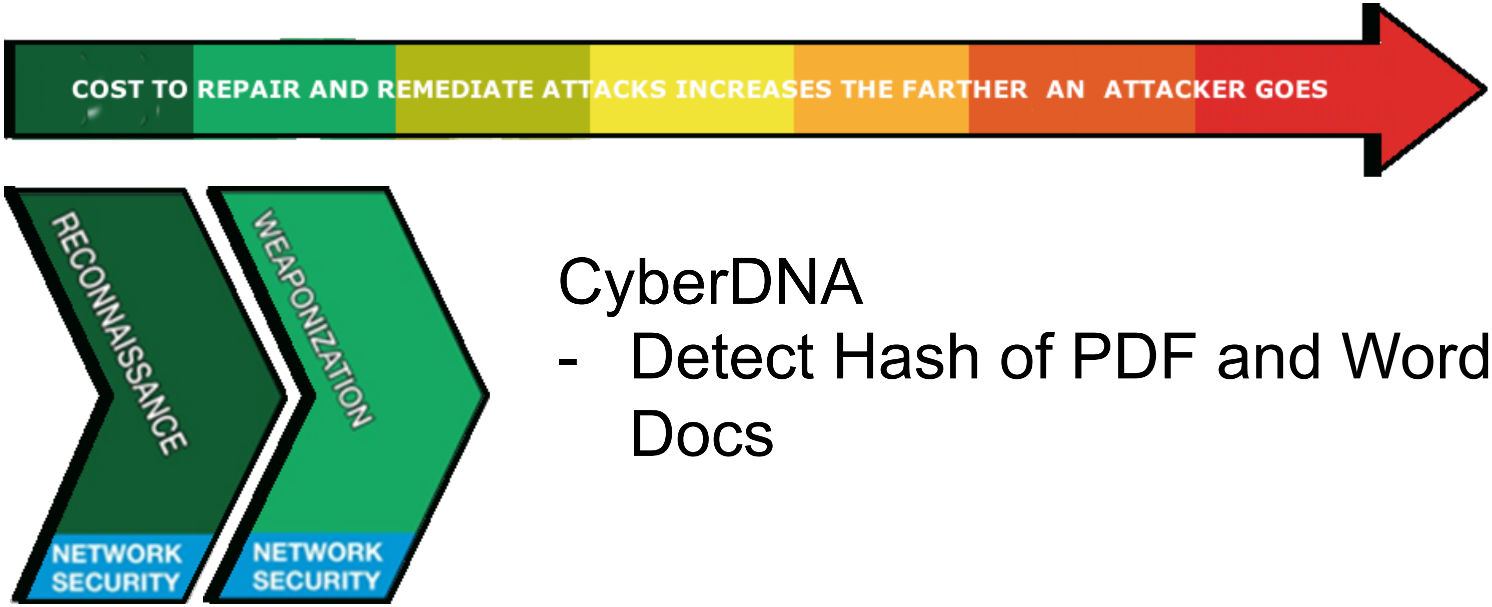
RECONNAISSANCE
NETWORK SECURITY

CyberDNA

- Watches / Correlates scanning
- We can also help reduce footprint

Lockheed Martin Kill Chain ®

Lower Your Costs - Use tools to Catch them early



COST TO REPAIR AND REMEDIATE ATTACKS INCREASES THE FARTHER AN ATTACKER GOES

RECONNAISSANCE

NETWORK SECURITY

WEAPONIZATION

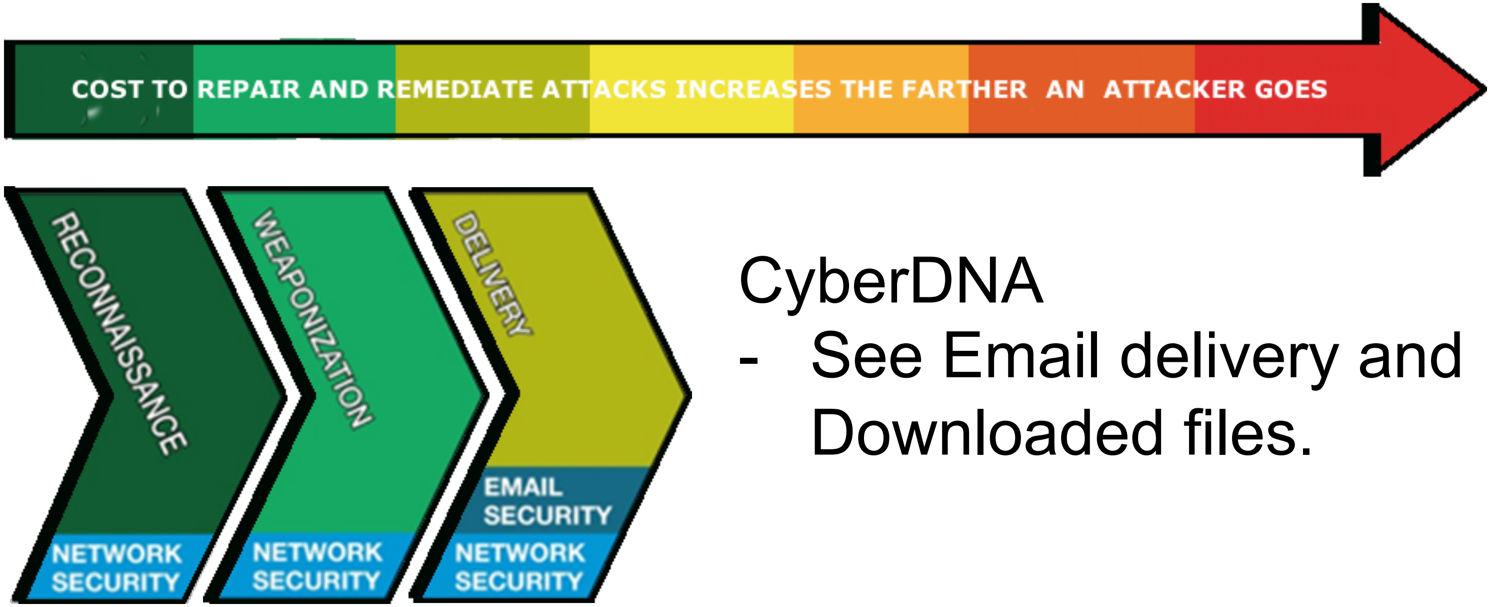
NETWORK SECURITY

CyberDNA

- Detect Hash of PDF and Word Docs

Lockheed Martin Kill Chain ®

Lower Your Costs - Use tools to Catch them early

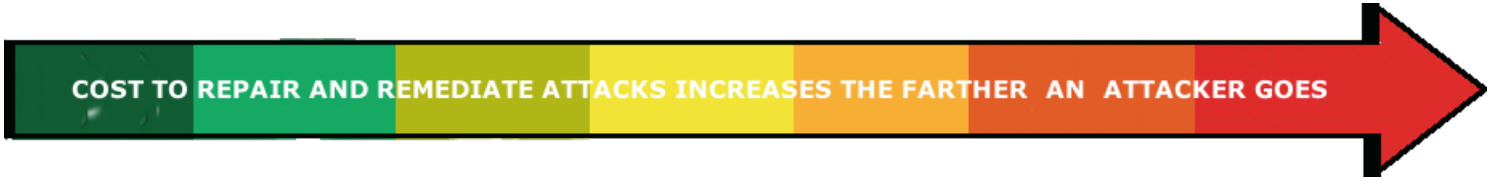


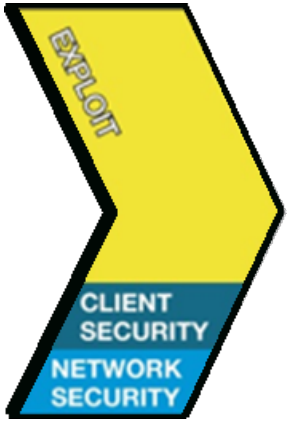
CyberDNA

- See Email delivery and Downloaded files.

Lockheed Martin Kill Chain ®

Lower Your Costs - Use tools to Catch them early


COST TO REPAIR AND REMEDIATE ATTACKS INCREASES THE FARTHER AN ATTACKER GOES

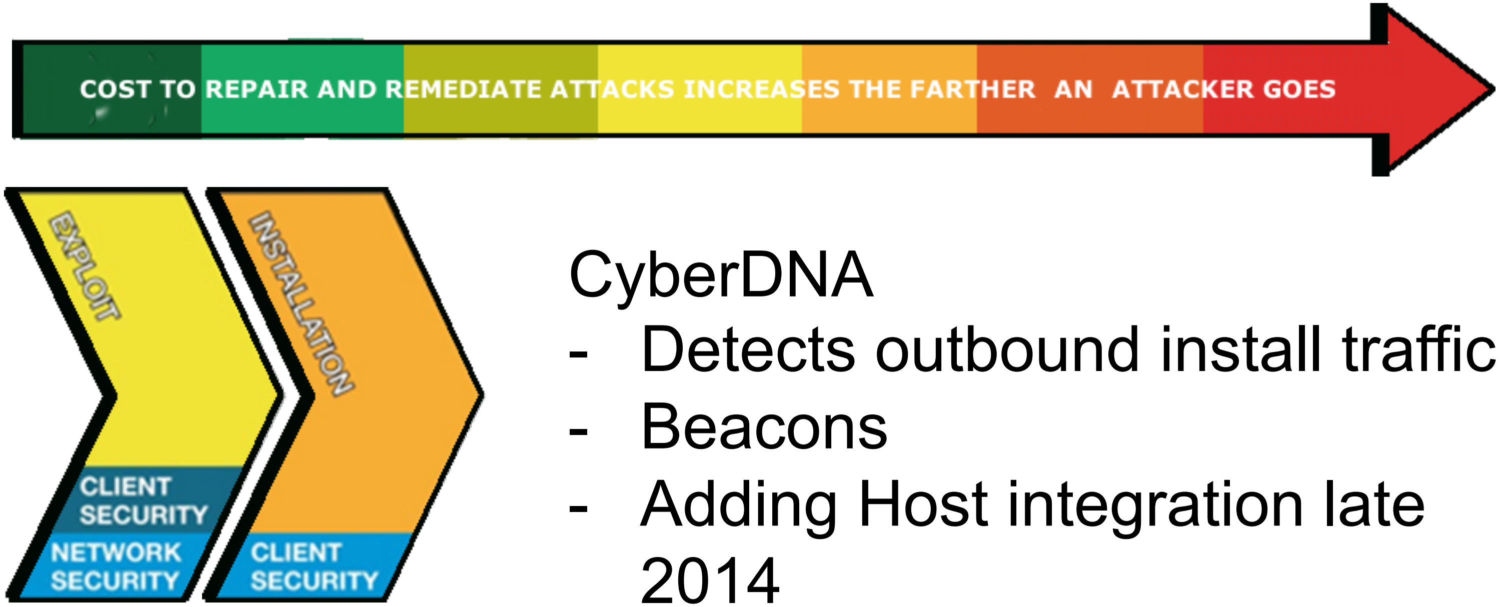


CyberDNA

- Exploit traffic rises above
- Detects code passing through network traffic

Lockheed Martin Kill Chain ®

Lower Your Costs - Use tools to Catch them early

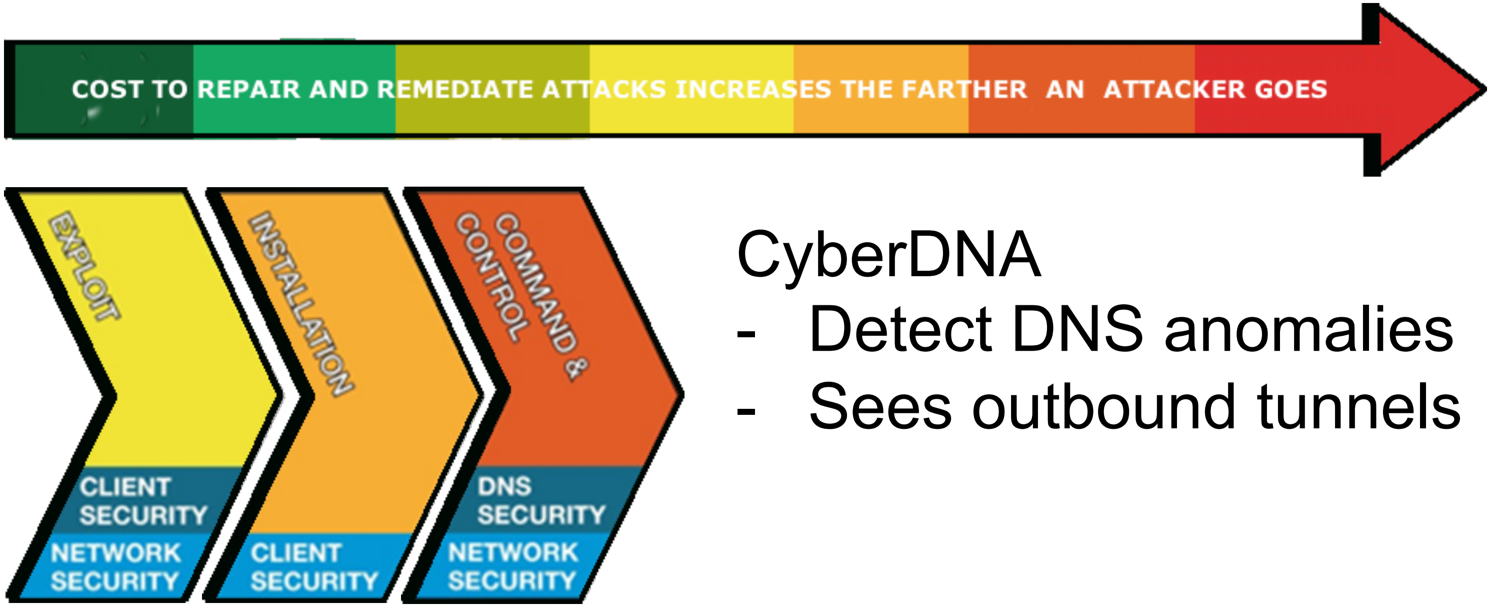

COST TO REPAIR AND REMEDIATE ATTACKS INCREASES THE FARTHER AN ATTACKER GOES
EXPLOIT
CLIENT SECURITY
NETWORK SECURITY
INSTALLATION
CLIENT SECURITY

CyberDNA

- Detects outbound install traffic
- Beacons
- Adding Host integration late 2014

Lockheed Martin Kill Chain ®

Lower Your Costs - Use tools to Catch them early

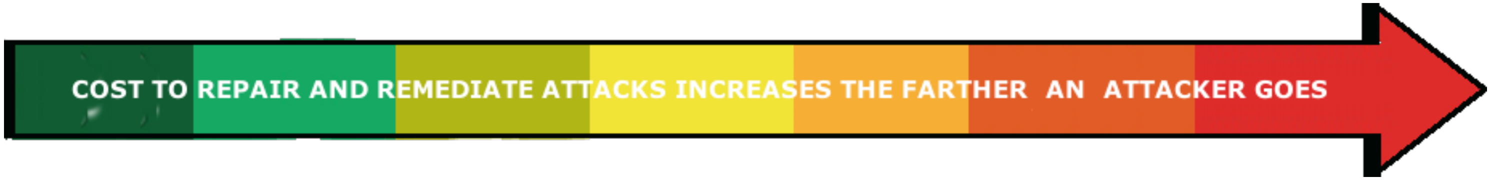


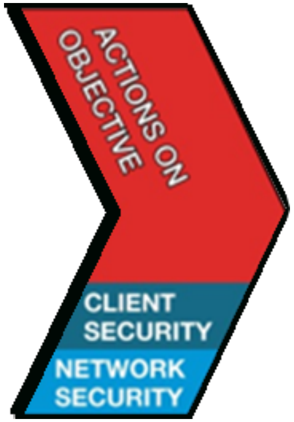
CyberDNA

- Detect DNS anomalies
- Sees outbound tunnels

Lockheed Martin Kill Chain ®

Lower Your Costs - Use tools to Catch them early


COST TO REPAIR AND REMEDIATE ATTACKS INCREASES THE FARTHER AN ATTACKER GOES



Action on Objective is most expensive

- Full Packet Capture and replay attack
- Know Who, What, When and Where

Lockheed Martin Kill Chain ®

Take Away #5
Use Layered Protection

- Have solid perimeter defenses
- Use AV and Signature Detection
- Most importantly teach your internal team on secure use of internet.
- Second most important: Use Anomaly Based detection
- Have Focused IT Security Staff or Managed Services

What we covered:

- Understanding the Problem - Compliance and Security
- How attacks have changed and the Security industry hasn’t
- Lower your exposure and breach costs

Five Take Aways

1. Security is not the same as Compliance
2. SMB is the new gateway – Protect your reputation you may be the path
3. AV is dead does not make you safe it is only a layer of protection and not a good one.
4. Act like they are already in – Anomaly and Passive detection is imperative
5. Lower breach costs - Use Layered Protection and find them fast.

VIGILANT
TECHNOLOGY SOLUTIONS
WWW.VIGILANTNOW.COM - SALES@VIGILANTNOW.COM

CyberDNA

KNOW WHEN

KNOW WHERE

KNOW HOW

Chris Nyhuis
cnyhuis@vigilantnow.com
http://www.vigilantnow.com