Mitigate Breach Damages with Real-time Analytics using Time-based Security

About The Speaker

I'm Gary S. Miliefsky, Cyber Security Expert.
Inventor. Entrepreneur. Frequent Speaker
Publisher of Cyber Defense Magazine
My bio is online at: www.garymiliefsky.com

AS SEEN IN

THE WALL STREET JOURNAL.
The New York Times
CNN THE AGENCY POST
Entrepreneur MAGAZINE
The Washington Post
Chicago Tribune

abc CBS FOX FOX NEWS CTV NEWS
NBC CNN MSNBC
WMUR 9
sky NEWS
BOSTON HERALD RADIO TALK IT UP!

Today's Agenda

Mitigate Breach Damages with Real-time Analytics using…

Time-based Security

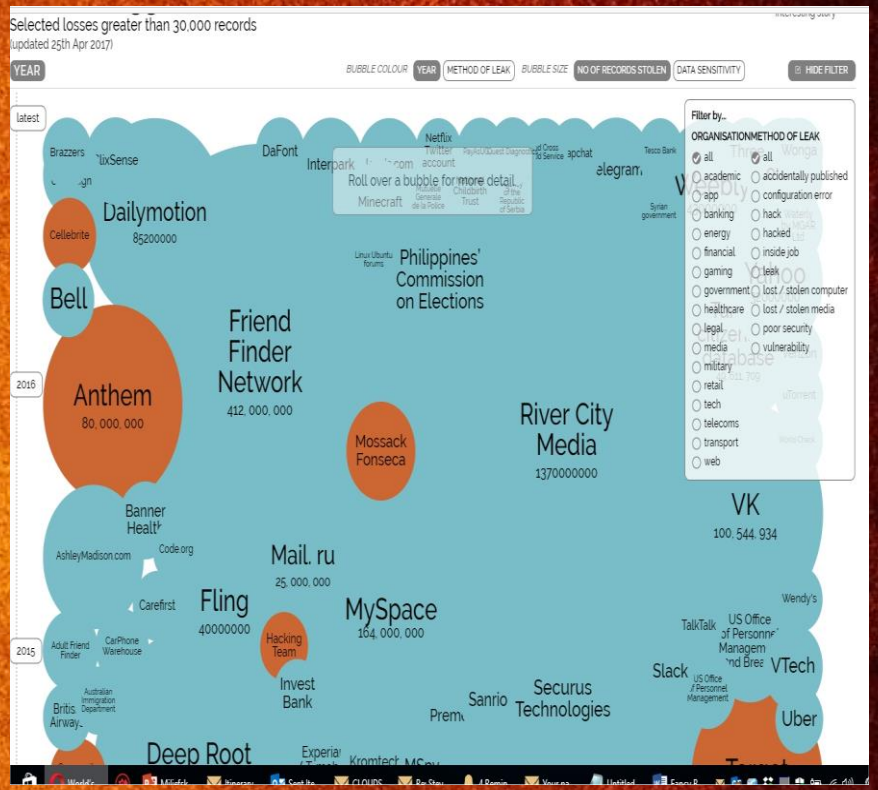
How Bad Are The Breaches?

Please take the time to visit a visual mapping of the largest breaches…

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Which I shortened for you…

https://tinyurl.com/threatbook2017



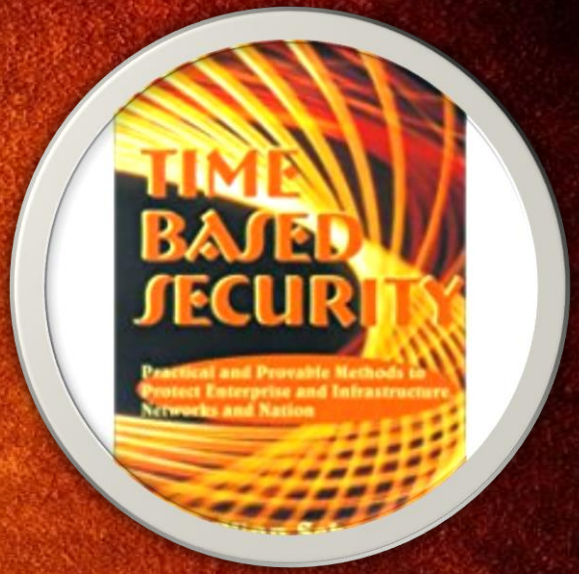
BILLIONS OF RECORDS, SO FAR…

Breaches Happen in a Window of Time

If We Understand
Time-Based Security,
We Might Be Able to Get One Step
Ahead of the Next Threat…

What is Time-based Security (TBS)?

- Discovered and written about in 1999 by my past advisor and friend, Winn Schwartau.
- A methodology that a security officer can use to quantifiably test and measure the effectiveness of security measures.
- TBS Gives us a measurable foundation for Stopping Breaches!



Time-based Security (TBS) Formula

Pt > Dt + Rt

Protection time needs to be greater than the Detection time plus the Response time

Time-based Security (TBS) Corollary

Pt < Dt + Rt

If it takes longer to detect and respond to an intrusion than the amount of Protection time afforded by the Protection solution, P, then effective security is impossible.

Real-world Example of TBS

Bank Robbers…

Bank Robbers

Real-world Example of TBS

Pt = It takes the burglars 8 minutes to get into the vault and 2 minutes to get into their getaway car.

Dt = In the first minute, the teller presses the silent alarm to call the police.

Rt = The Police are on their way and arrive in 11 minutes.

Time-based Security (TBS) Formula

Pt > Dt + Rt

10 min < 1 min + 11 min

Robbers get away!!! Failure.

Let's Catch Them This Time...

Add two factor authentication to the vault. (takes 30 seconds longer to open)

Require a second set of keys to open the vault from the manager who has an office on the far end of the building (takes him a minute and a half to walk to the vault)

Move the Bank Branch closer to the local police department (takes them 9 minutes to arrive)

Time-based Security (TBS) Formula

Pt > Dt + Rt

12 min > 1 min + 9 min

Robbers arrested before they reach the front door of the bank on their way out. We win!

Bank Robbers Arrested

Can We Do The Same for INFOSEC?

Assuming we have the best training, techniques and tools in place (Encryption, Good Key Management, Authentication, Firewall, Endpoint Security, SIEM) and real-time feeds like ThreatBook.

Let's look at our network from the perimeter to all the devices on the intranet. Now let's:

Measure Dt + Rt (sec/min/hrs/day)

Can We Do The Same for INFOSEC?

Now we can proactively measure the following:

- Time to detect an event?
- Time to respond to an event?
- How much damage can be done in Dt+Rt?

So How Can We Beat The Threat?

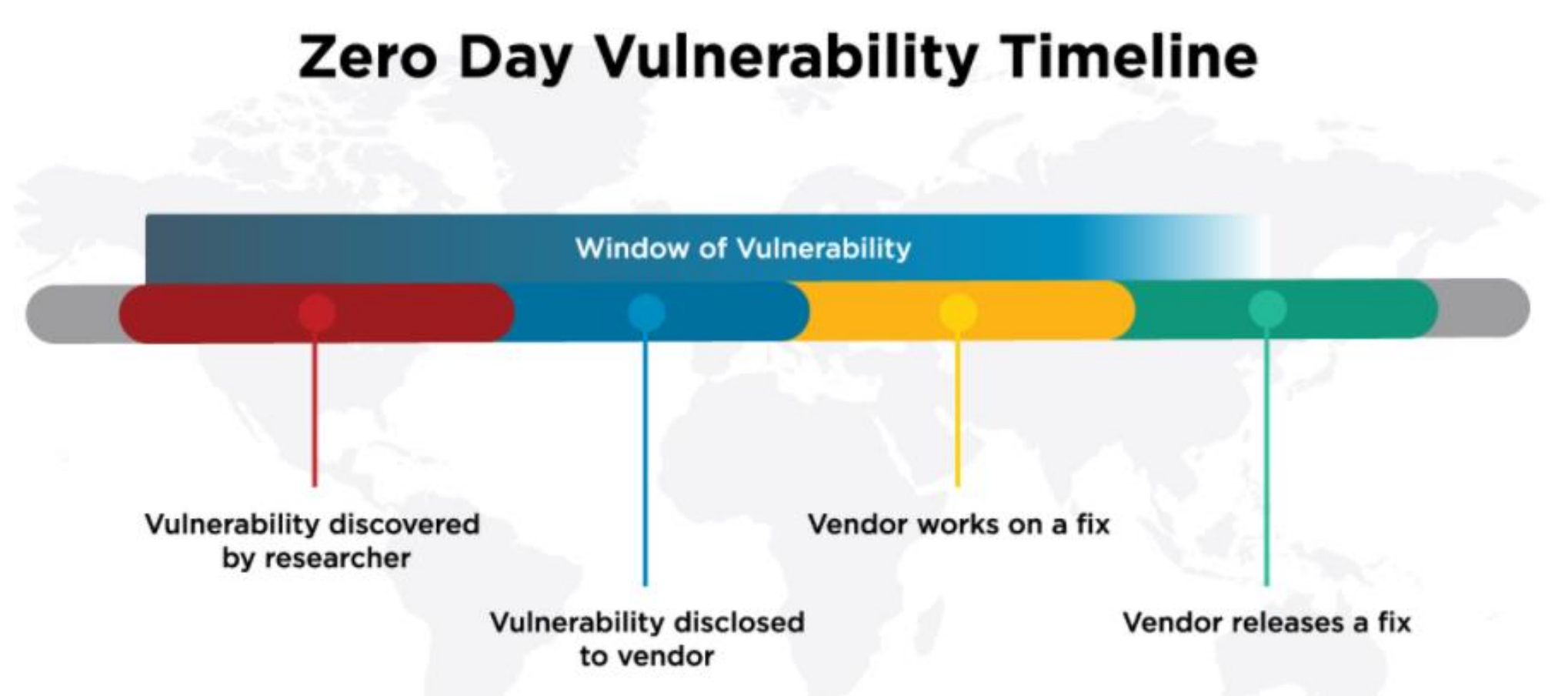
It's all about Exposure Time

$$Et = Dt + Rt$$

We need to minimize Exposure Time or at least make it smaller than the time it takes to complete the Exploitation and steal our Confidential Data

Exposure Time is The...

Window of Vulnerability



We Must Go Faster or...

Breaches must go slower.

How To Make Breaches Go Slower...

VMs & HoneyPots, Bandwidth Limiting, Data Padding and Stronger Encryption Everywhere

Slowing Down The Breach, Example…

HoneyPots at the Perimeter (provides a DECEPTION layer)

Example: Dt = 12 minutes

Hacker spends at least 14 minutes or more in the HoneyPot exploiting holes and stealing fake data and is detected during that time, before they can reach and exfiltrate the real critical data.

Slowing Down The Breach, Example...

Data Padding:

Pad the critical files so their size exceeds the Exposure time (Et).

Example:

Et=10 min, Bw=6 Gb/hr.
File Size = (1/6 hr) / (6 Gb/hr) = 1 Gb
Therefore, all critical files should be padded to be larger than 1Gb.

Going Faster Means...

We Need Real-time Analytics by Coupling Human Intelligence, Artificial Intelligence and Machine Learning.

Mitigating Breach Damages…

We must be faster than the exploiter.

Hence, Real-time Analytics is so important.

Mitigating Breach Damages...

T x V x A

Threats x Vulnerabilities x Assets

Real-time Analytics

What are the latest and newest Threats? Are we being attacked or exploited by any of them right now?

What are the most serious Vulnerabilities (CVEs)? Do we have any of them?

Where is the critical data? What Assets are the most valuable? How are we protecting them?

Mitigating Breach Damages...

Leveraging Real-time Analytics around these key variables:

Threats x Vulnerabilities x Assets

We must know all of our threats as quickly as possible. We must know all of our serious or critical vulnerabilities as quickly as possible and understand the correlation between an exploiter or threat and the vulnerabilitity they are attempting to exploit. Finally, we must track, control, manage and value all of our network assets, especially those that host or manage critical and confidential data.

Reducing Detection time (Dt) by Defending Against Exploitable Holes

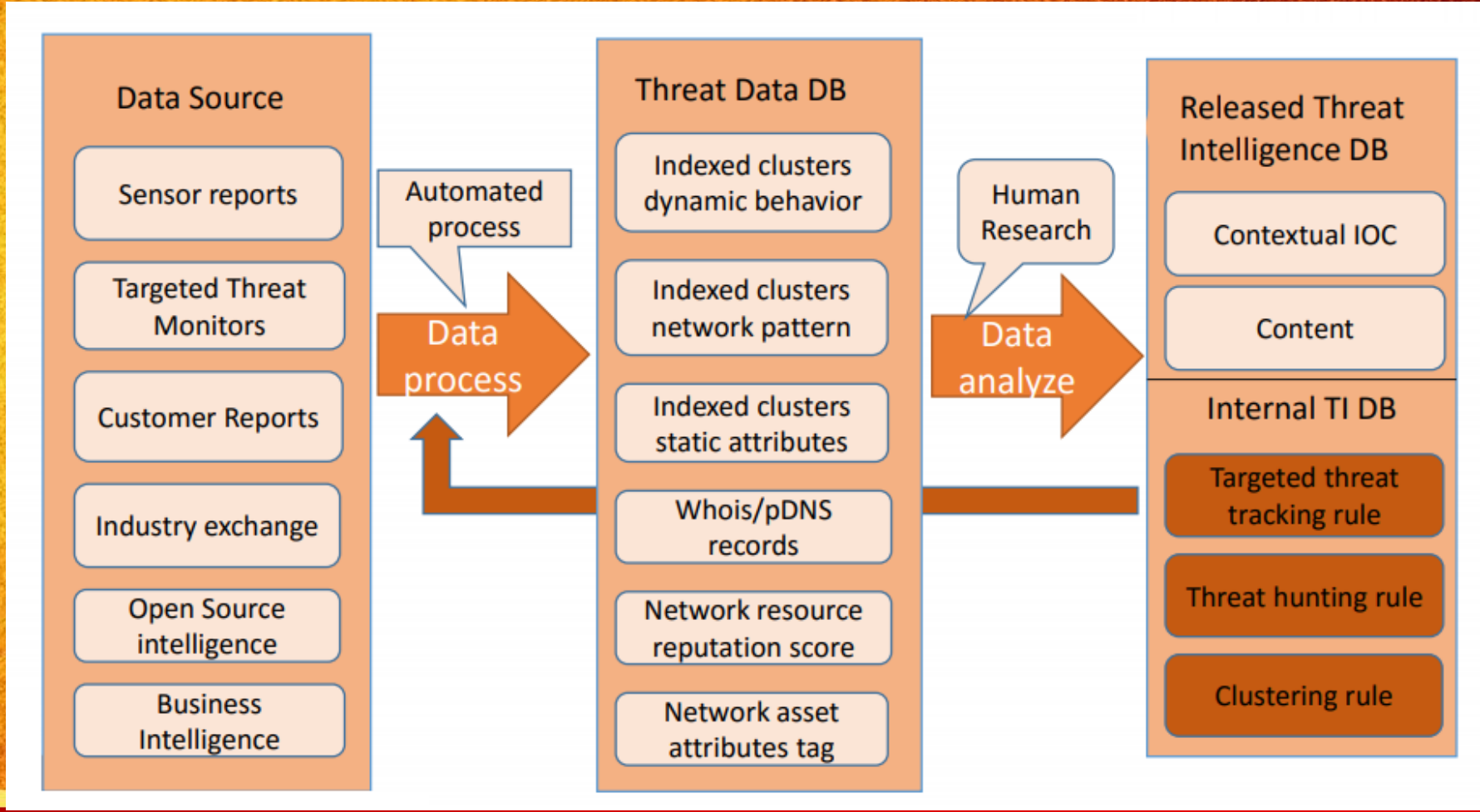
Remediation can be done in these key ways:

Use a CVE auditing system from vendors like Trend Micro, Qualys, Rapid7, Tenable, etc. or try open source OpenVAS...

Patch the holes that can be patched. Test the patch.

Reconfigure the system when no patch is available (close the port, turn off the service, disable admin account, etc.)

Reducing Detection time (Dt) Using Best of Breed Tools Like ThreatBook…



Mitigating Breach Damages…

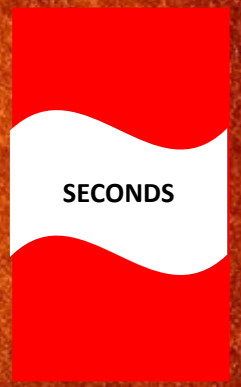
We've lost the data
278 days

Current Average Detection time (Dt) According to FireEye

We're losing the data
15 minutes

Today's Best Practices Detection time (Dt) with SIEM & Orchestration

We've saved the data
2 seconds or less



Tomorrow's Time-based Security with Machine Learning & AI and Proactive Defenses

In Summary

The smaller we can make the Detection time plus the Response time …ie…

Dt + Rt should be as close to zero as possible

The higher probability we cannot be breached and if we are breached, the data cannot be exfiltrated fast enough to cause harm or require regulatory compliance reporting.

Q&A

Free Resource

www.cyberdefensemagazine.com


Thank You!