Post-breach Response: Current and Future Response Capabilities

John South
December 11, 2014

Heartland

How were we breached?

Very Late 2007 – SQL Injection via a customer facing web page in our corporate (non-payments) environment. Bad guys were in our corporate network.

Early 2008 – Hired largest approved QSA to perform penetration testing of corporate environment

Spring 2008 – CEO learned of Sniffer Attack on Hannaford's , Created a dedicated Chief Security Officer Position and filled that position

April 30, 2008 – Passed 6th Consecutive "Annual Review" by Largest QSA

Very Late 2007 – Mid-May 2008 – Unknown period but it is possible that bad guys were studying the corporate network

Mid-May 2008 – Penetration of our Payments Network

Heartland

The Breach and the Announcement

Late October 2008 – Informed by a card brand that several issuers suspected a potential breach of one or more processors. We received sample fraud transactions to help us determine if there was a problem in our payments network. Many of these transactions never touched our payments network.

No evidence could be found of an intrusion despite vigorous efforts by HPS employees and then two forensics companies to find a problem.

January 9, 2009 – We were told by QIRA that “no problems were found” and that a final report reflecting that opinion would be forthcoming.

January 12, 2009 – January 20, 2009 – Learned of breach, notified card brands, notified law enforcement and made public announcement.

Heartland

Reaction

PANIC

DENIAL

ANGER

BARGAINING

DEPRESSION

ACCEPTANCE

FIX THE PROBLEM

Heartland

Lessons Learned from the Heartland Breach

Doing the “right thing” is not always the “right thing” – it’s all in the definition of “right”

At the time of breach, Heartland was fully compliant with existing Payment Card Industry Data Security Standards (PCI DSS). But….

Security without intelligence is a significant challenge

If you want to go fast, go alone. If you want to go far, go together (African proverb).

- Our competitors had information that could have protected us
- Established an organization of competitors to share what we were all seeing

Honesty above profit

Heartland

Security's secret weapon

As we go into 2014, we are developing a strong secret weapon for combatting cybercrime

- One part – shared intelligence (competitors are sharing pertinent attack data
- One part – better understanding of malicious actors, how they operate and their tactics, techniques and procedures (TTP)

Need two more parts

- Tools to protect the merchant and data from malicious activity
- Visualization of the threats

Heartland

Security’s secret weapon

Technology

Heartland

Minimalist Security in 2014

Stepping back……

Establish a security framework as a base

Religiously build security program around framework

- Architecture components
- Logging
- Penetration testing / vulnerability testing

Focus on software development environment

- Emphasize secure coding practices
- Extend penetration testing / vulnerability testing

Incident Response

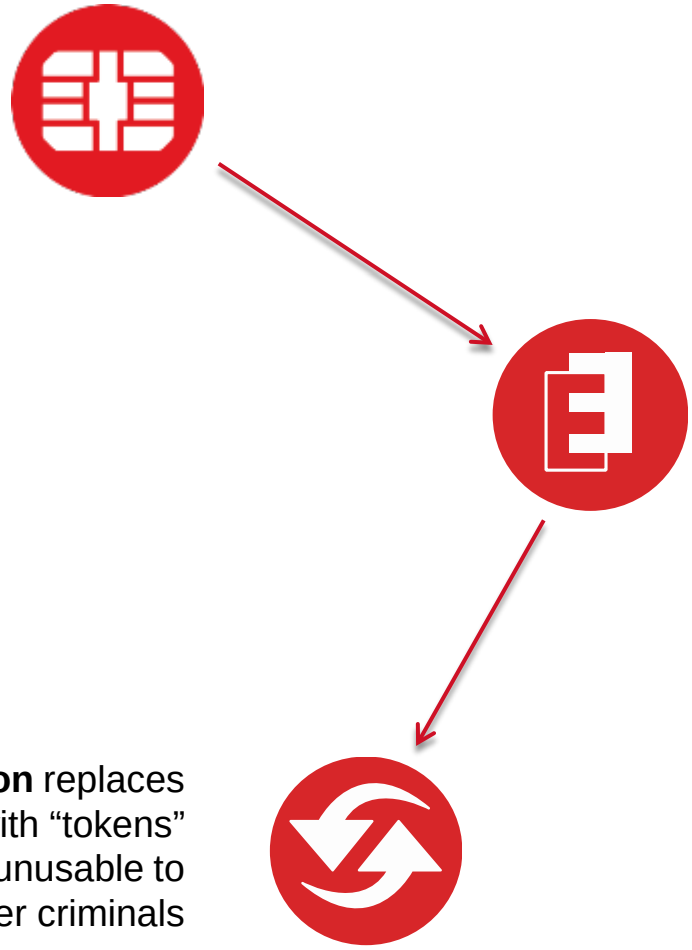
Business Continuity Management

Risk Management

Heartland

Technology to secure of data

EMV chip card technology improves security by providing card authentication



P2PE
end-to-end encryption technology encrypts card data at inception

Tokenization replaces card data with “tokens” making it unusable to cyber criminals

Heartland

So, fraud is stopped!!! ☺

Well……not exactly

Currently in the US, the level of payment card fraud is about 6 basis points

In Europe – 6.3 basis point

So what did we accomplish in Europe?

Effectively, we relocated fraud from Card Present to Card Not Present

EMV stopped counterfeit card transactions, but the Walmart, Home Depot, etc attacks were NOT about the use of fraudulent cards IN the store.

So, will the shift to the new technologies “solve” the problem?

What is the economic burden of imposing EMV on our merchants?

Heartland

Security’s secret weapon

Visualization

Heartland

Minimalist Security in 2014

Do all of this and you should afford yourself a good portion of security
But….you are not immune to attacks

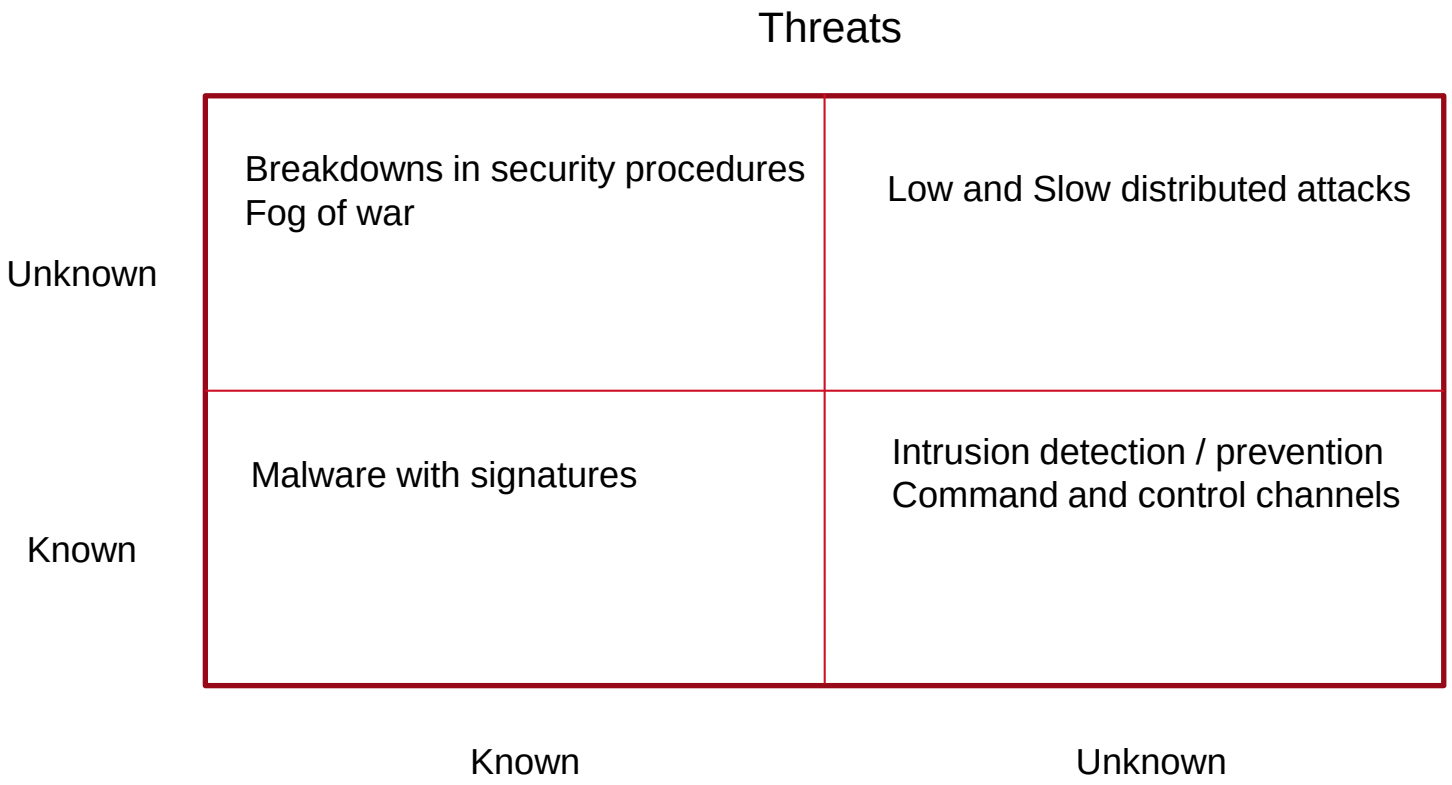
Why is that?

We are good at known knowns and known unknowns

What we are not good at is unknown unknowns

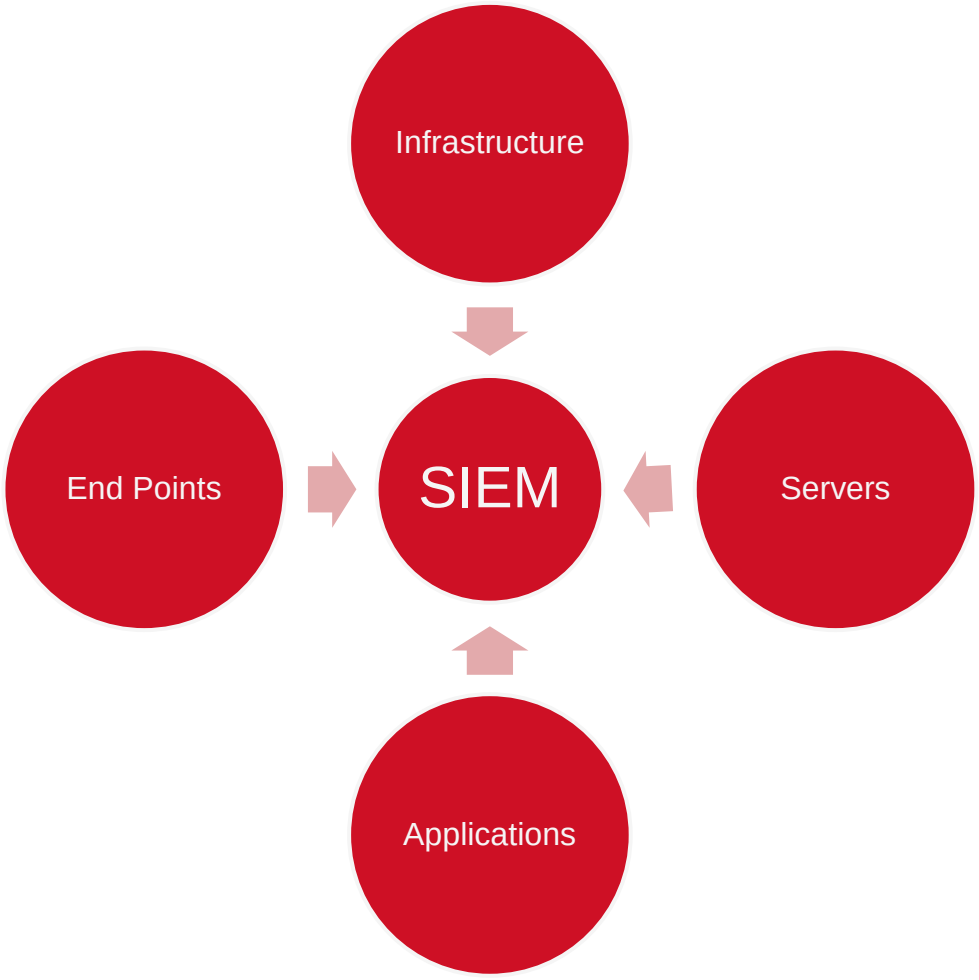
Heartland

Minimalist Security in 2014



Heartland

Scope of our problem



Heartland

Scope of Problem

In a small to medium-sized company

- 50 – 100 million security events logged to the SIEM every day

In a large company,

- 5 – 10 billion security events recorded to the SIEM every day

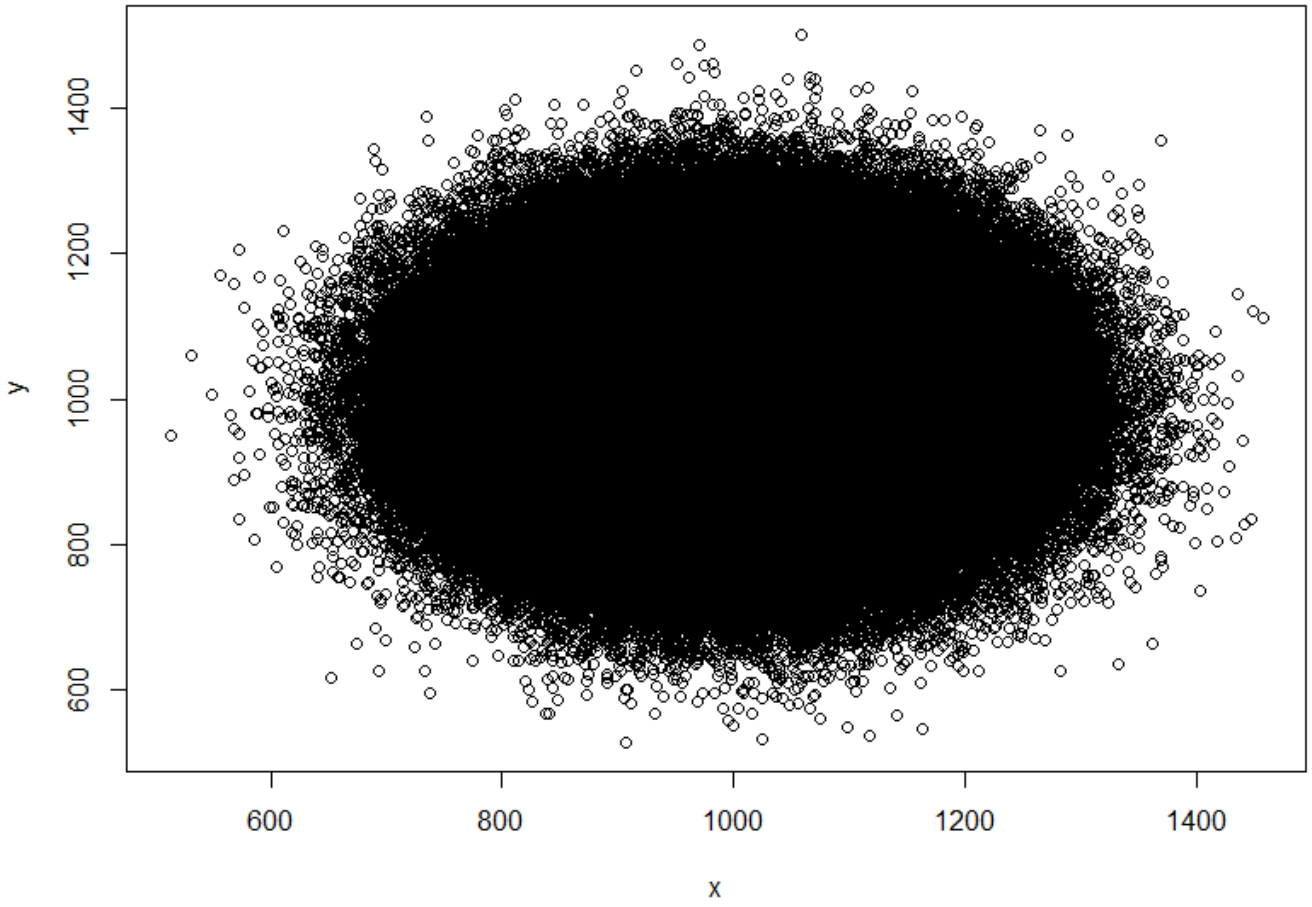
This is not a needle in the haystack problem

Rather, it is an eye of the needle in the haystack problem

Heartland

Scope of the problem

Simulation of 1,000,000 attack events

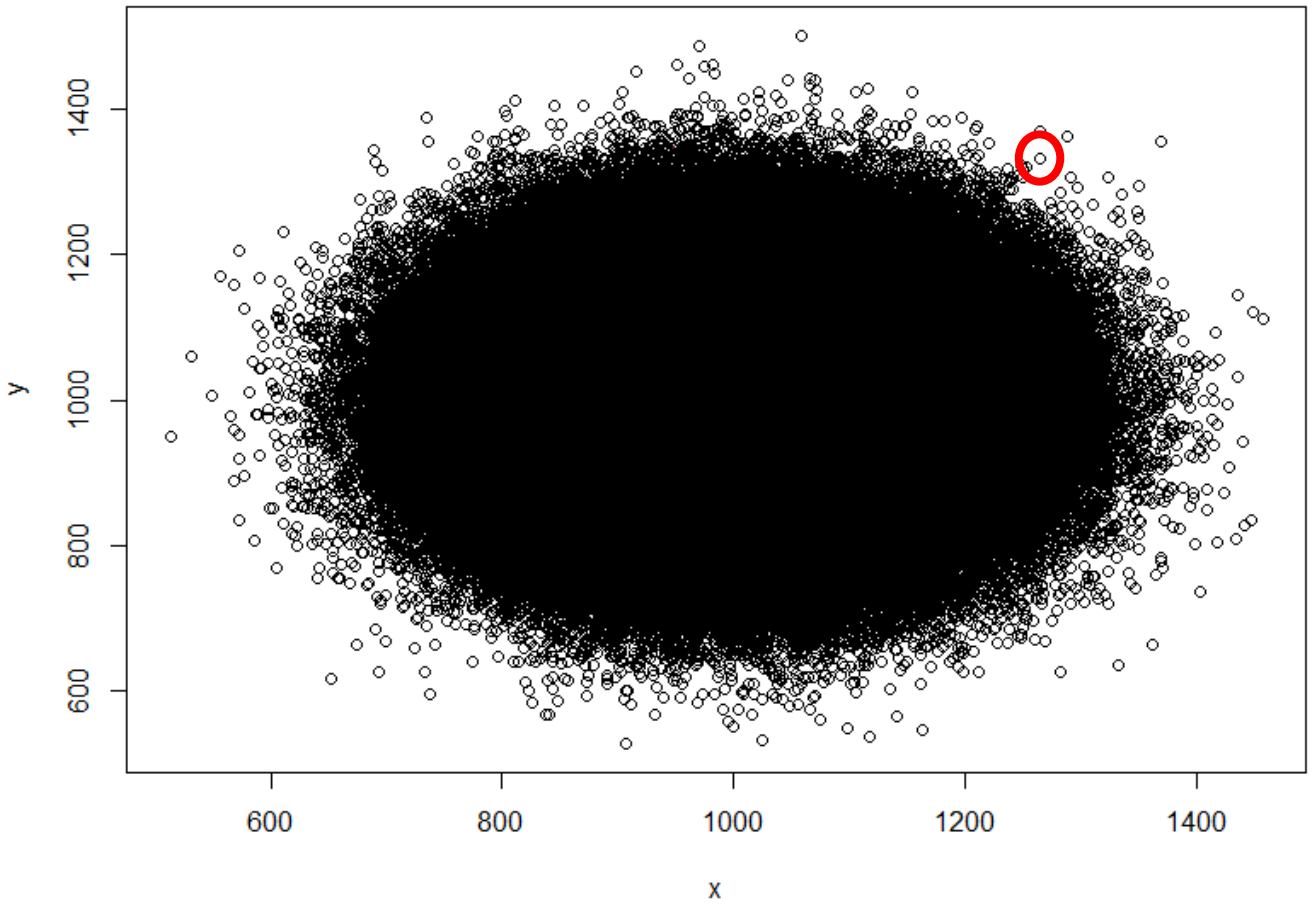


Random data
normalized,
Mean = 1000
s.d. = 100

Heartland

Scope of the problem

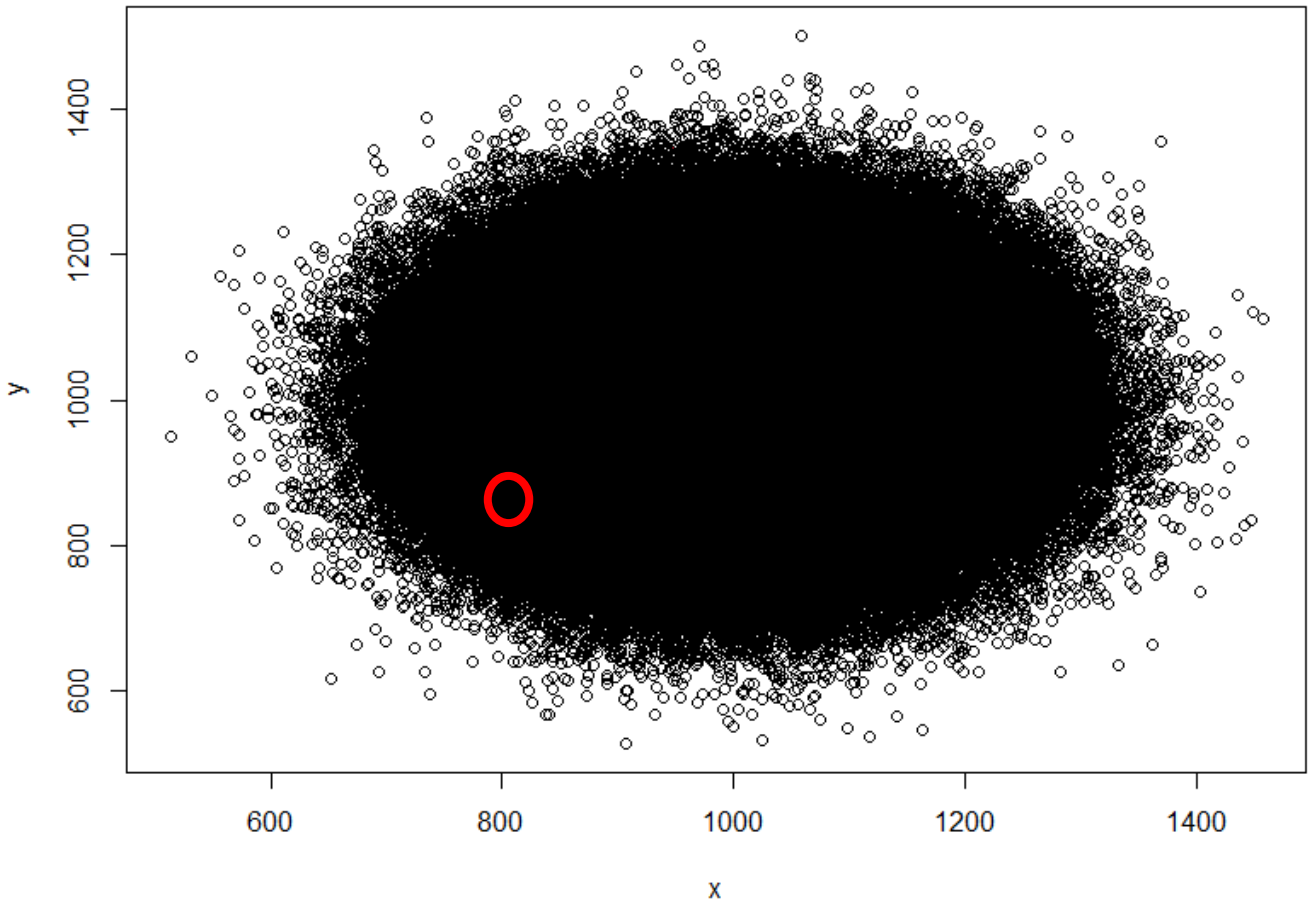
Simulation of 1,000,000 attack events



Heartland

Scope of the problem

Simulation of 1,000,000 attack events



Heartland

Visualization

Toolsets are getting better

We can have much better tools in 2014 to see problematic event patterns

Data analytics are beginning to play a larger role in the process of security

Lacking an effective use case where “big data” is actually making a difference in security, particularly for medium-sized company (scale issue)

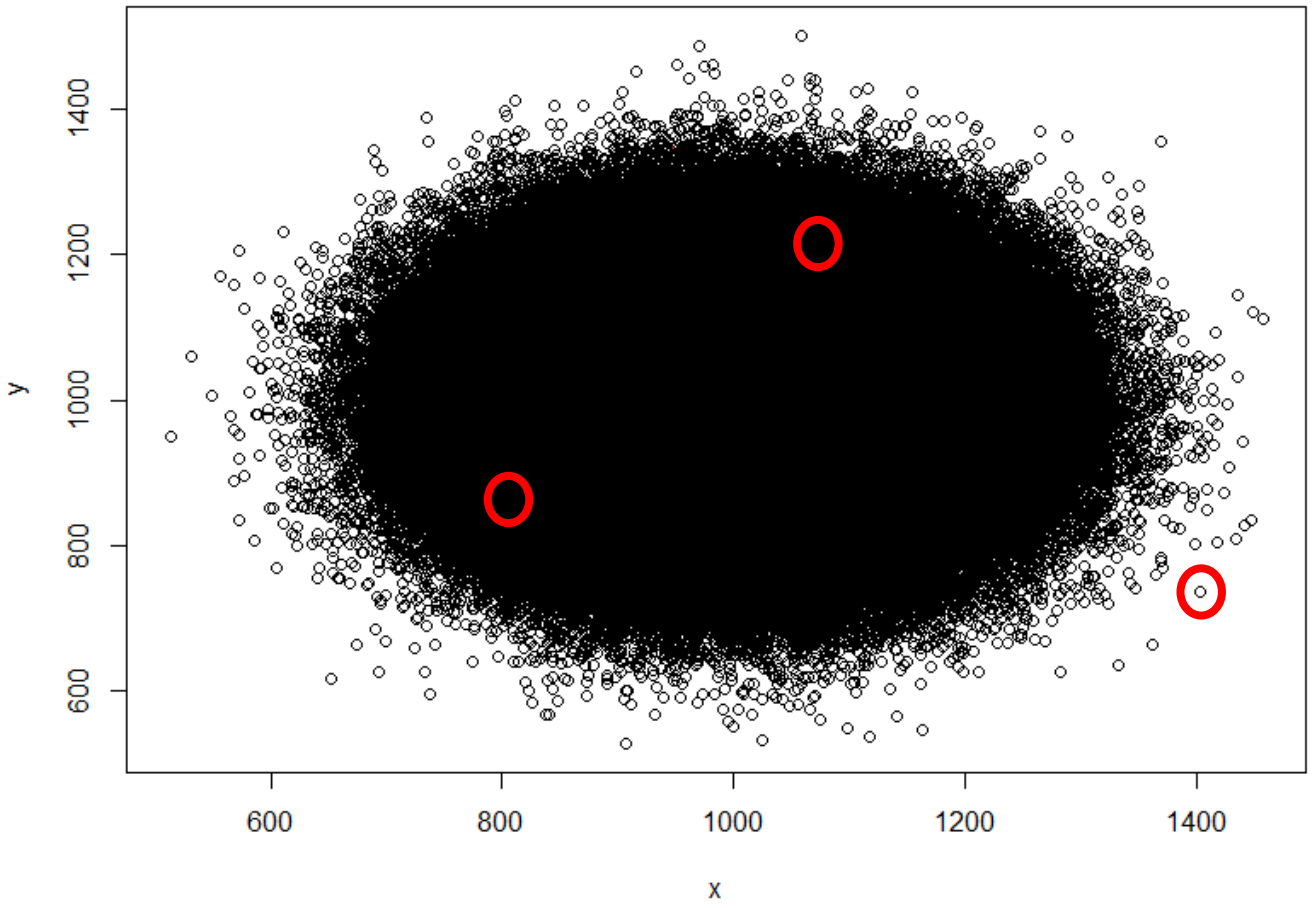
How do we identify and respond to long, slow distributed attacks – longitudinal analysis problems?

Emerging security practitioner as “data scientist”

Heartland

Scope of the problem

Simulation of 1,000,000 attack events



Heartland

Another secret weapon…

Effective Use of Auditing and Compliance

Heartland

Effective Use of Auditing and Compliance

Long-time axiom, compliance does not equal security

But, many companies still focus on compliance driven activities

Combined with the auditing function, we can more solidify our processes and procedures to encompass emerging sciences of data security

We understand how to audit compliance, but how do you determine if a SOC is effectively utilizing their longitudinal time analysis processes to detect distributed, slow and low attacks from China?

IT Security Auditor has to become proficient in understanding new threat vectors and detection methodologies, just as they did in understanding incident response

Today's risks are growing dramatically – none of us can afford to do business as usual

Heartland

In summary

We understand the process of security much better today than 5 -10 years ago

- We have better threat intelligence
- We've established common shared intelligence frameworks
- We understand the threats better than ever in the past

However, companies are still being breached – big and small

- Amount of data needed to protect a company is almost overwhelming
- Sometimes companies get defocused from their security initiatives
- Security teams are often buried three or four layers deep in their organizations

Data analytics and visualization of threat events is becoming more of a reality

- But the investment can be rather steep

We can, however, make use of auditing to assist in the process of effectively combatting our newest threats

Heartland