Security analytics: From data to action

Visual and analytical approaches to detecting modern adversaries

Chris Calvert, CISSP, CISM – Director of Solutions Innovation

My job is innovation so I own the buzzword slides

(Google trends report)

The security industry is not catching enough bad guys

Most enterprises remain challenged with missing critical breaches

229 days

is the median duration of how long breaches were present before discovery in 2013

(M-Trends Report)

100%

of business networks have traffic going to known malware hosting websites

(Cisco 2014 Annual Security Report)

Why is this so hard?

Bad guys know how to stay inside the bell curve.

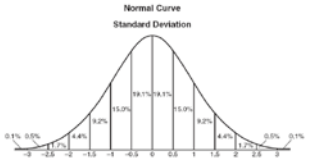
Known: Easier to detect

- Matches a signature
- Goes to a bad place
- Works in the clear
- Unauthorized use
- Outside of baseline
- Within monitored infrastructure

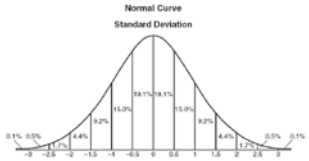
Unknown: Harder to detect

- New behavior
- Goes to an approved place
- Works encrypted
- Authorized use
- Inside of baseline
- Outside monitored infrastructure

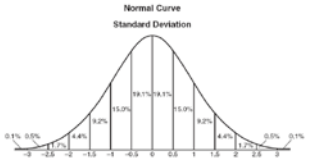
If hackers are challenging, then insiders are …



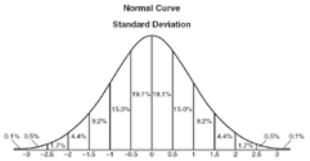
Source network



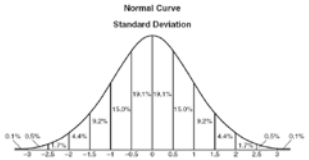
Time of day



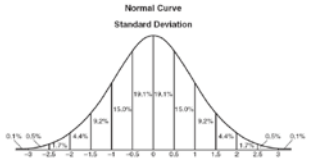
Day of week



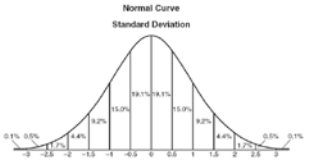
HR status



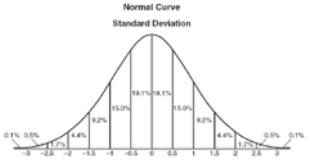
User identity



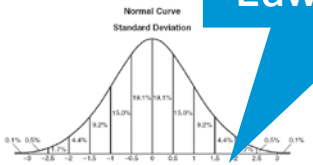
Target system



MAC address

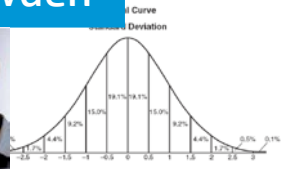


Geography



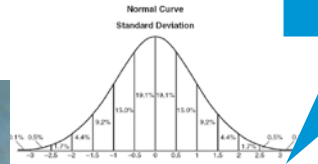
Sensitivity of data

Edward Snowden



Coworkers

Robert Hanssen

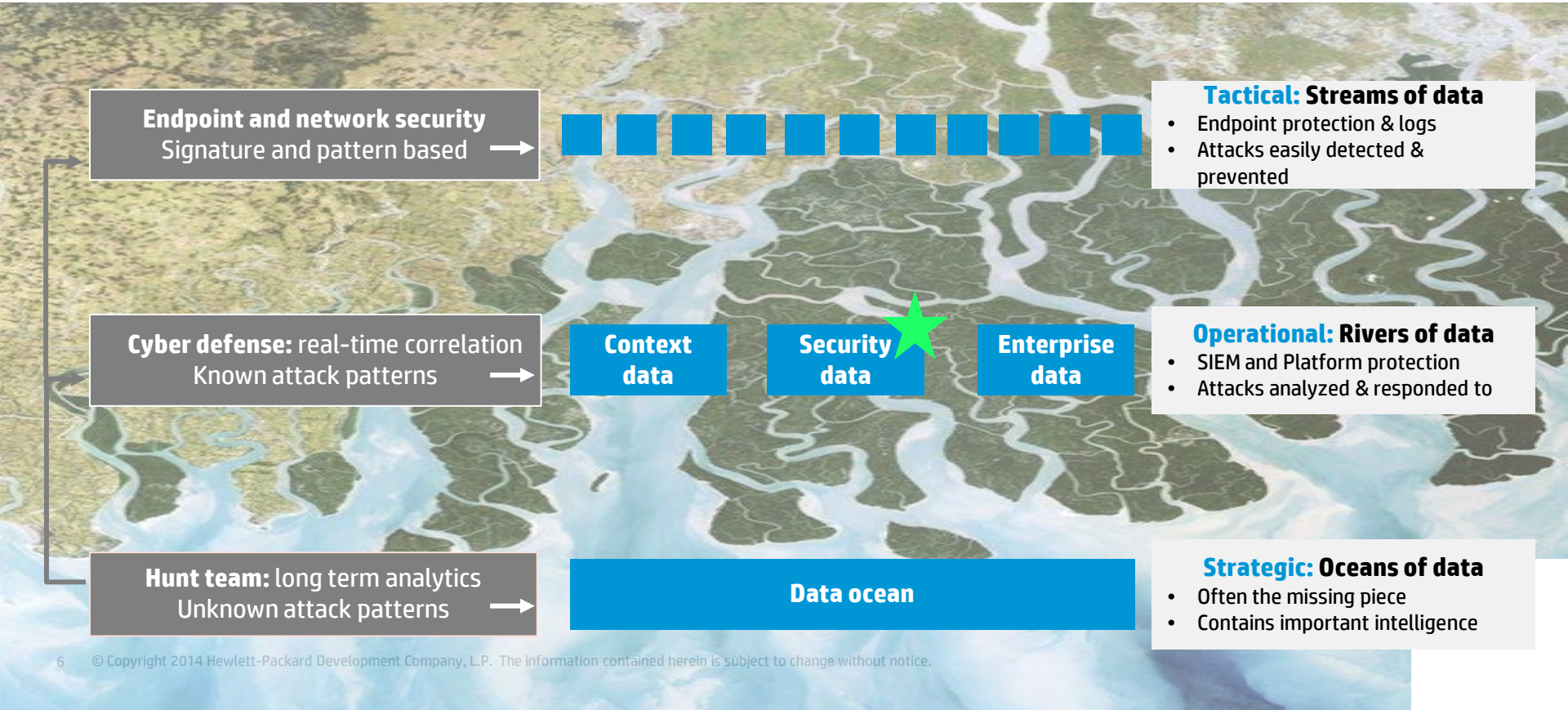


Lifestyle information

Aldrich Ames

The geography of security detection has changed

Data flows in many ways – where should we catch and analyze it?



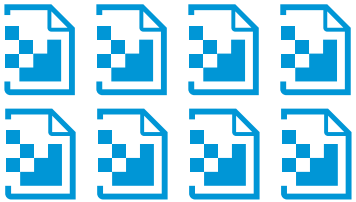
All data is not equal

The conventional wisdom of collect everything and figure it out later is **wrong!**

And expensive…

- $collect, $process, $analyze, $store, $manage

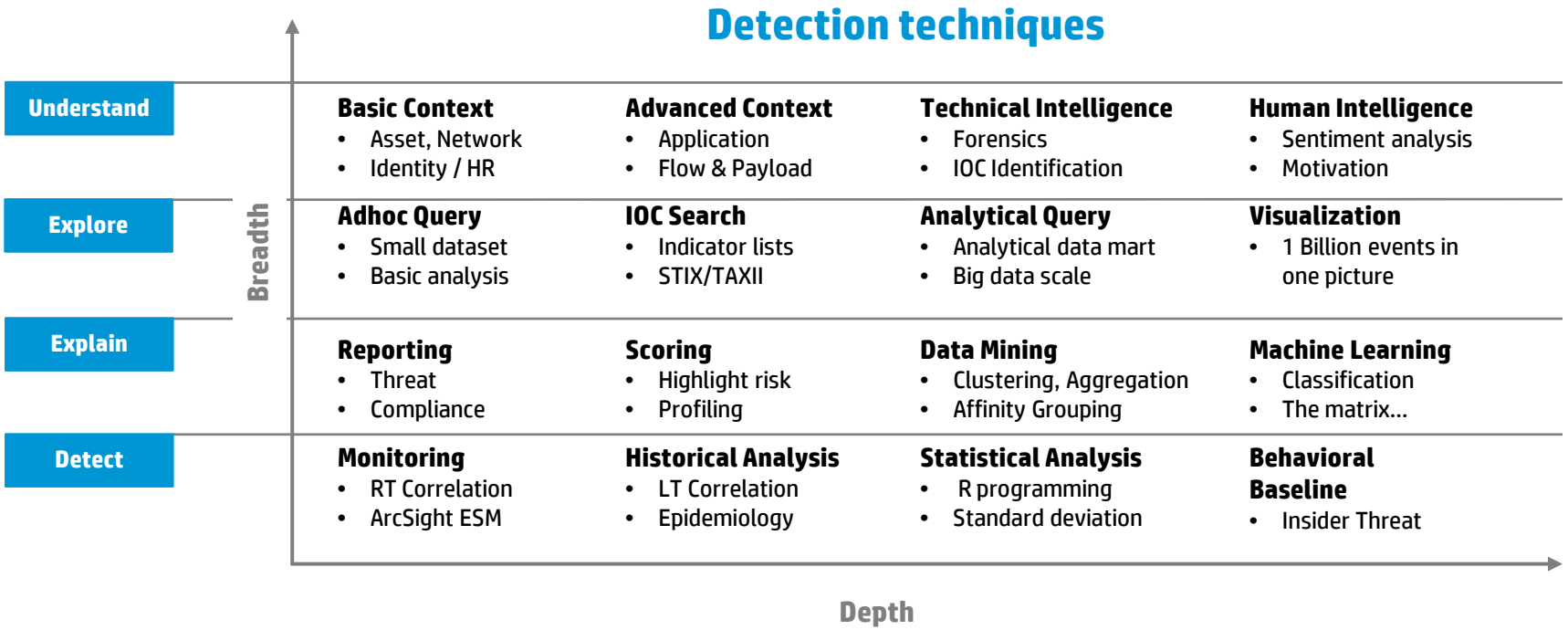
You should consider the small analytics problems first



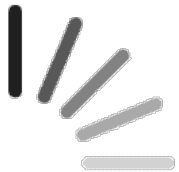
Collect what matters to solving a real problem – are all these logs useful?

We need to expand our detection capabilities

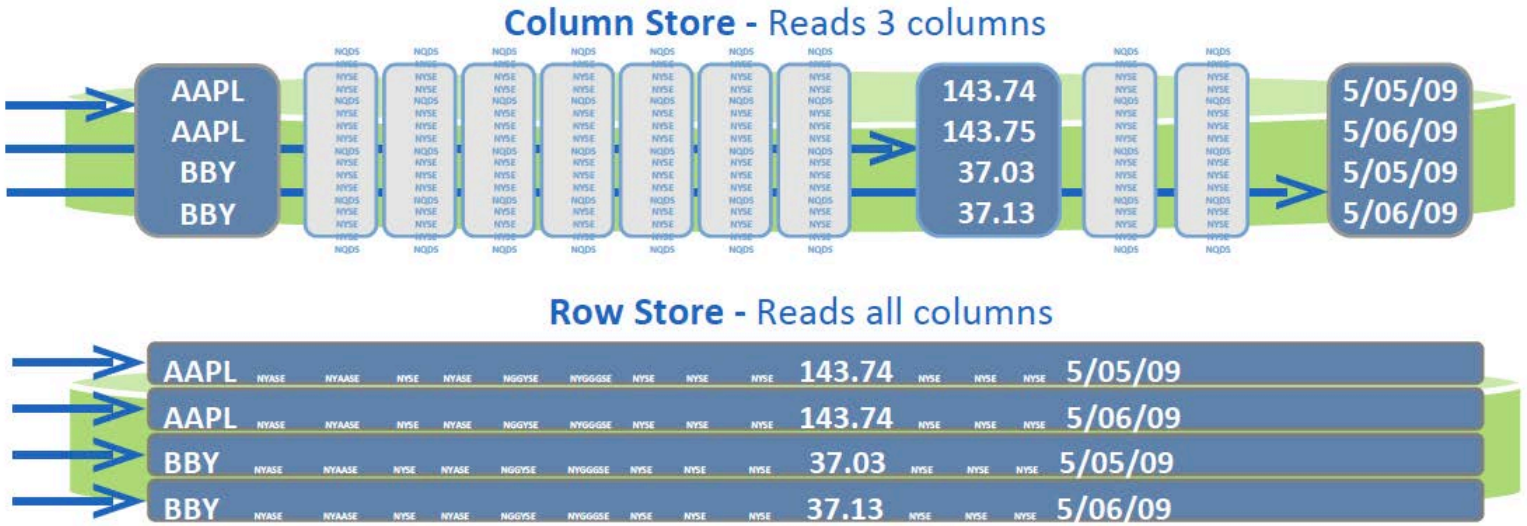
Adding advanced analytics to detection is critical to the future of security.



What stopped us from this kind of analysis?



Analytics of the future relies on columnar retrieval



Compression

Clustering

Distributed Query

Find needles and understand haystacks using…

Disciplines of analytics

Classification - context (asset model, etc…)

Correlation - real-time (ESM) and historical

Clustering – common root cause

Affinity Grouping - relationships in data

Aggregation - assemble attacker profile

Statistical Analysis – reporting and anomalies

Visualization of big data – affinity group

This example reveals a command and control infrastructure

Business statement

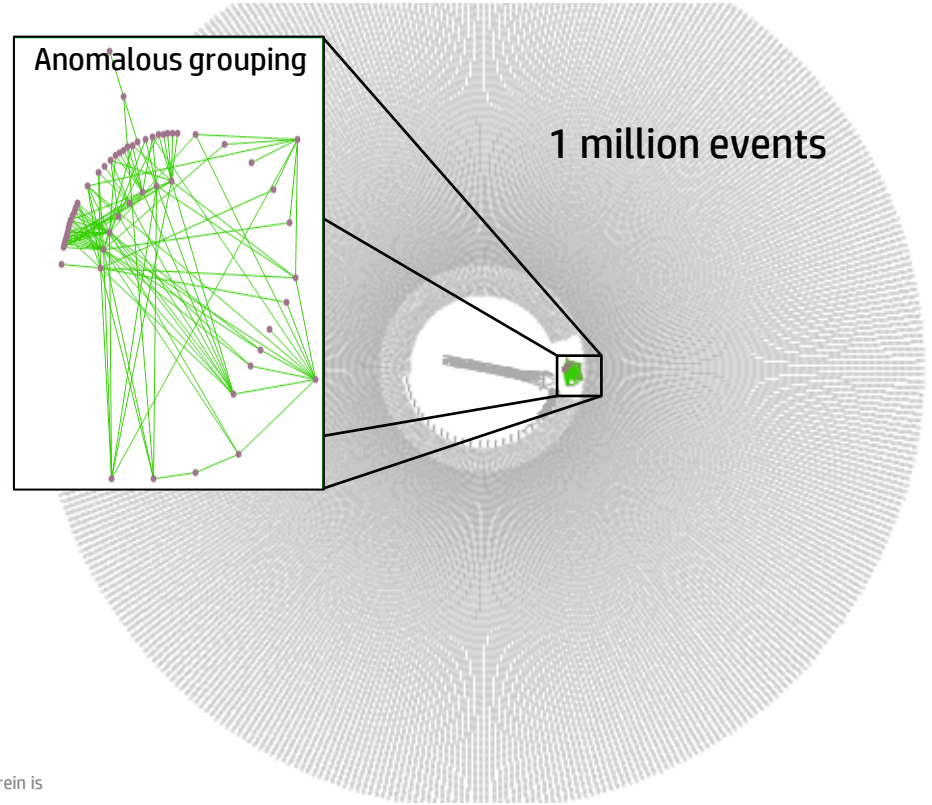
- Find **command and control infrastructure** in your enterprise

Analytics statement

- Identify **affinity groups**
- Investigate anomalous groupings

Findings from visualization

- Hierarchical, highly-resilient C&C infrastructure



Visualization of big data – scatterplot

This example reveals a low and slow scan

Business statement

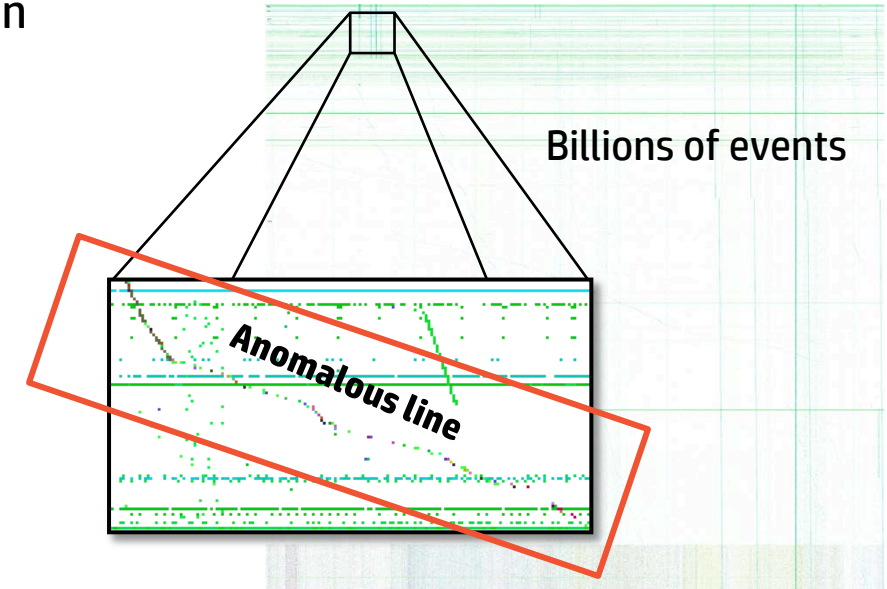
- Find sophisticated port scan activity (distributed, randomized)

Analytics statement

- Plot multiple months of data on one scatterplot

Findings from visualization

- Single multi-week scan from distributed, internal sources indicates advanced attacker



Visualization of big data – anomaly chart

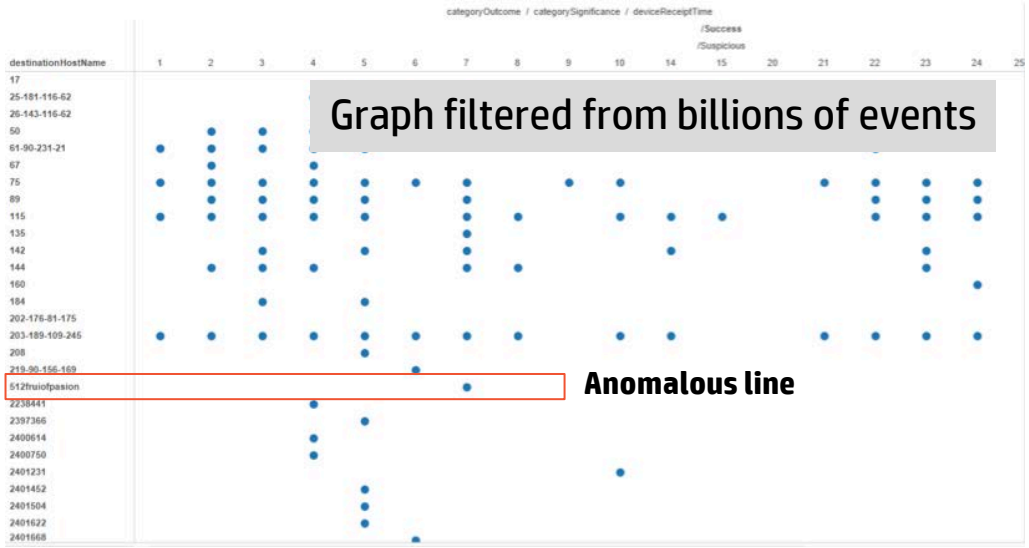
This example reveals inappropriate communication **(bottom 10 phenomenon)**

Business statement

- Find servers talking to suspicious hosts outside the network

Analytics statement

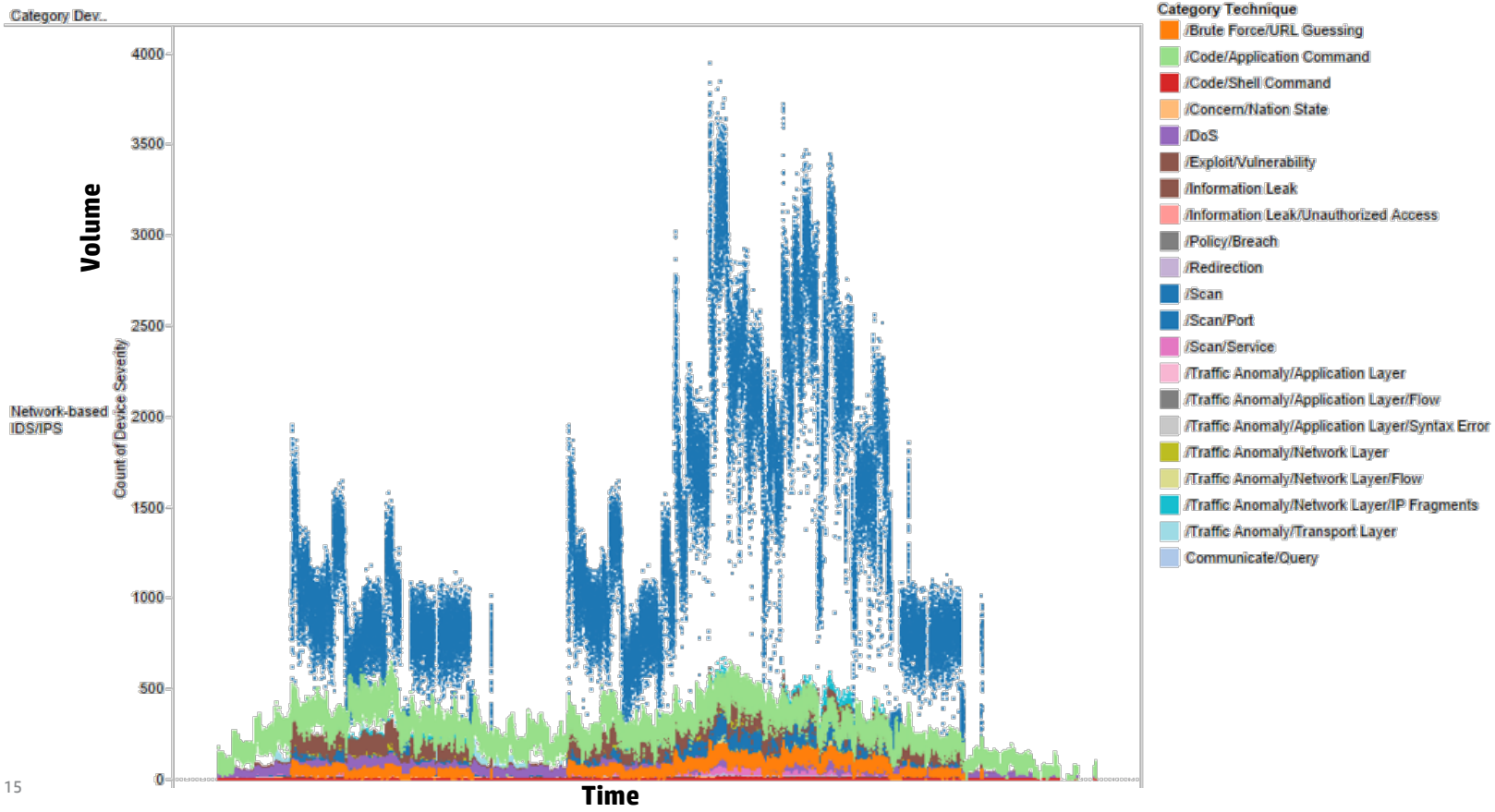
- Plot all suspicious successful communications and review



Findings from visualization

- A host communicated w/ suspicious external website
- Unique in that no other host in the environment has ever talked to this external website

Analyzing the haystack – aka reporting

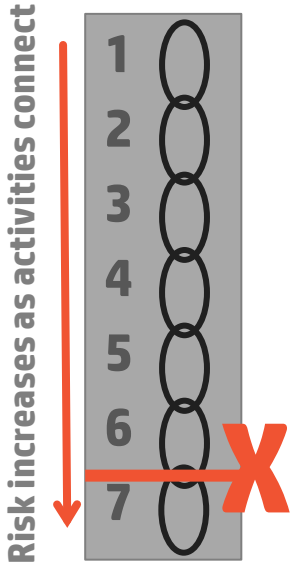


The holy grail – predictive analytics

Analysis can help you determine behavioral chains to find the next expected event

If you can determine typical steps in a breach, fraud or attack life-cycle

You can introduce actions to monitor or block the activity following the behavior



We know this is hard! Yet none of this is possible without big data and analytics. You are building capabilities that can grow with the **maturity** of your security program.

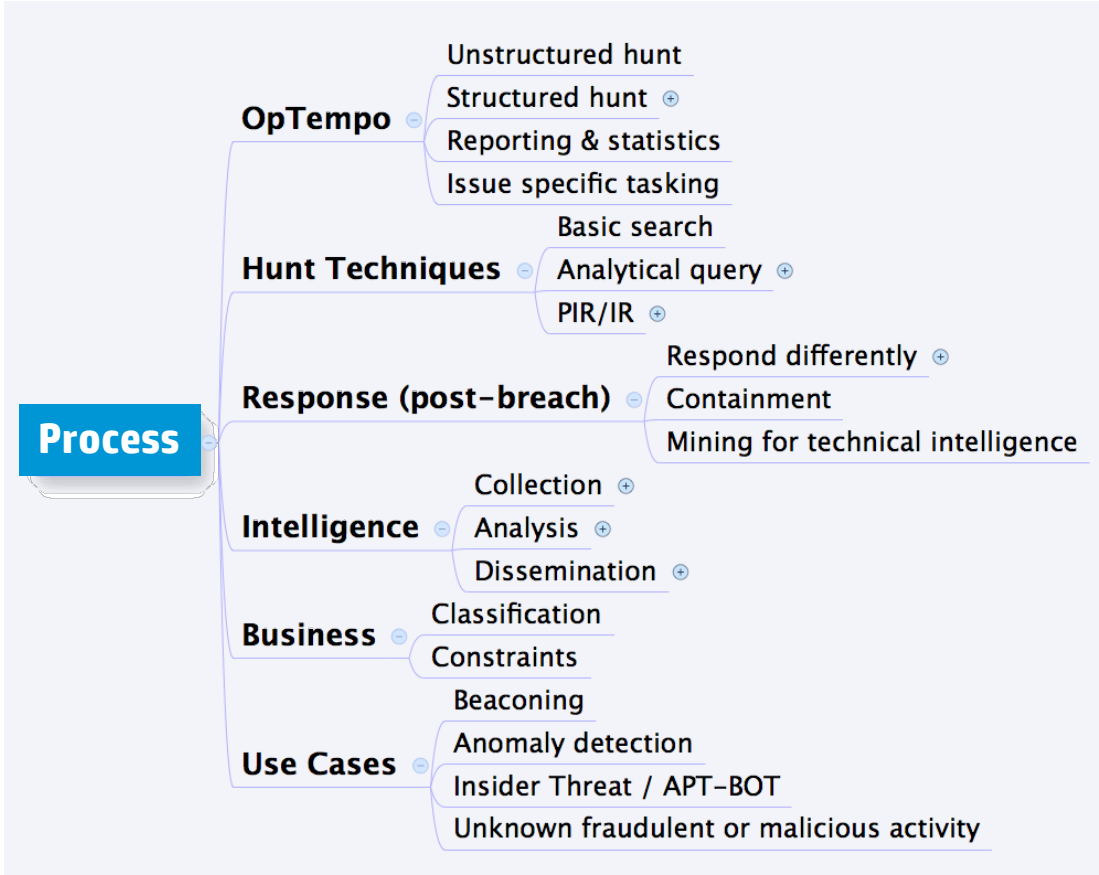
Security analytics = exploration

http://h30499.www3.hp.com/t5/HP-Security-Products-Blog/Important-Questions-for-Big-Security-Data/

Data exploration is key!

- Explore!
- Ask adhoc **questions**
- Refine data mart (query or side table)
- Develop repeatable solution
- Drive events back to ESM
- Explore some more

Hunt team – the way to operationalize analytics



Your hunt team needs a 2-sided skill set

Roles and personas

Security specialist:

- The “go to” person to get to the bottom of any major security incidents and would be responsible for actively hunting for indicators of breach
- This person understand and researched hyper-current attacker tactics, techniques and procedures

Data scientist:

- Knowledgeable to run specialized queries. Tasked to regularly find interesting anomalies or affinities in the data to review with the security specialist.
- This person optimizes tooling/searches, finding patterns that can increase risk probability factors and finding common patterns in attacks.

They’re in there!
Let’s find them.

For more information

Speak to our experts

- Chris.Calvert@hp.com
- Jeff.McGee@hp.com

After the event

- Contact your sales rep
- Check out our blog: hp.com/go/securityproductsblog

Your feedback is important to us. Please take a few minutes to complete the session survey.

Please give me your feedback

Session TB3272 **Speaker** Chris Calvert

Please fill out a survey.

Hand it to the door monitor on your way out.

Thank you for providing your feedback, which helps us enhance content for future events.

Thank you

Make it matter.