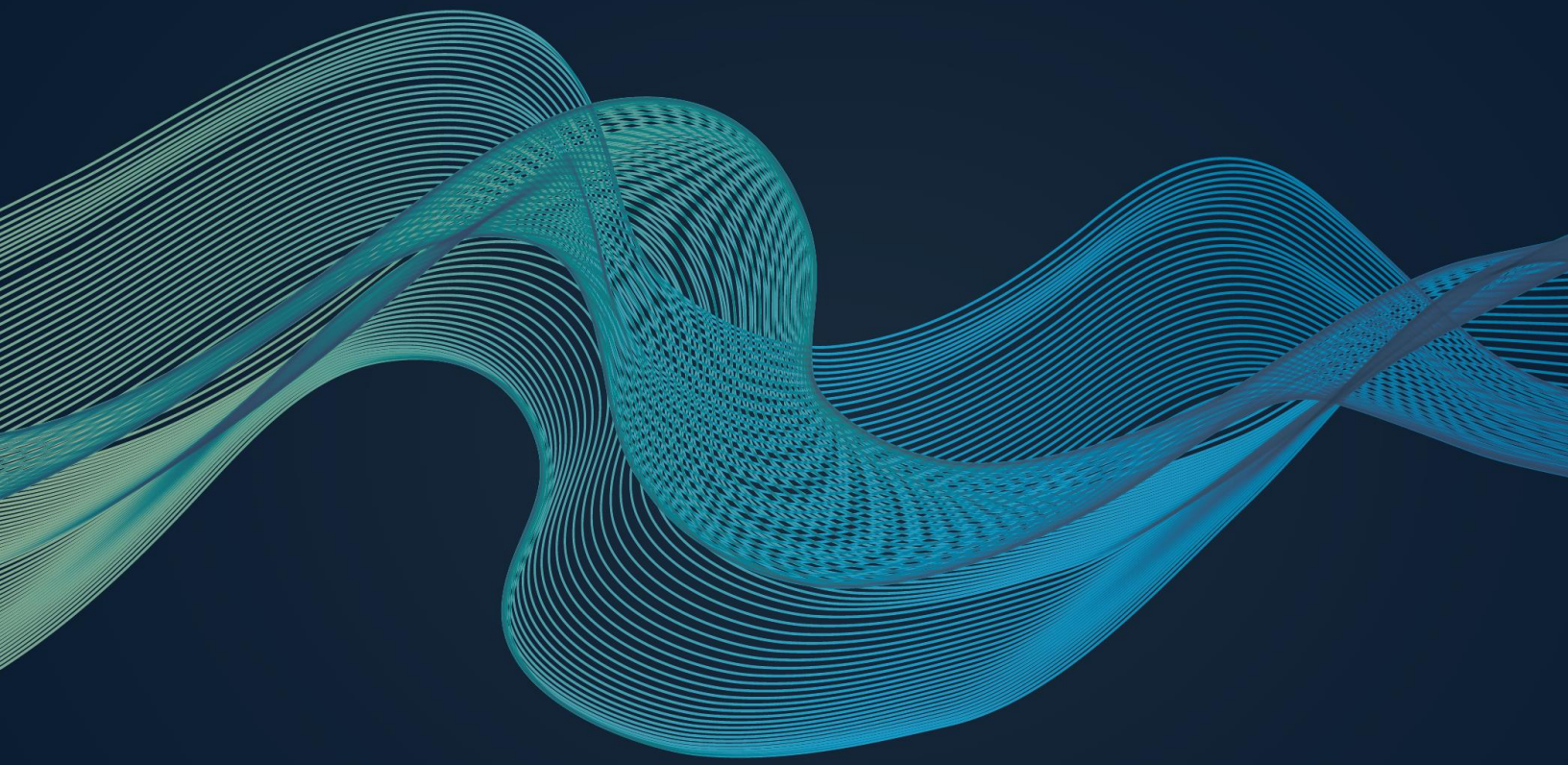
Big Data, Big Mess:

Sound Cyber Risk Intelligence through “Complete Context”



SURFWATCH
CYBER IN SIGHT

Introduction

When it comes to cybersecurity, perhaps nothing has been as highly touted as the answer to every executive's prayers as big data. It makes sense. Cybercrime, being inherently technical, can provide vast droves of data to be analyzed, and for years the drum has been beaten that big data will change the world.

But years after "big data" became just another marketing buzzword, organizations are still grappling with the issue of how to use that data in a practical way.

In fact, an interesting backlash is underway in 2014. In March, Google Flu Trends, which had been held up as the poster child for how big data could improve the world, was shown to have been consistently wrong in its flu predictions, in some cases more than doubling the actual figure compared to the Centers for Disease Control and Prevention. This led to a number of headlines about the problems with big data, its failings, and how all that data could lead to "gigantic mistakes."

But those bold headlines missed the more nuanced view of the problem.

As The New York Times reported, the best analysis didn't come from either the CDC or from Google Flu Trends. It came from an amalgamation of the two: big data plus real-world insight working together.

It's the same with cybercrime. Data is useful, but only if it's being properly interpreted and conveyed. The problem isn't with data, but with the way in which people are using it. Simply put, data alone is missing context.

Big Data Needs "Complete Context"

Much has been made of the sheer amount of data that's available. That's one thing everyone can agree on, and even though security professionals are drowning in a flood of data, that flood will soon grow into a tsunami.

- In 2013 it was reported that 90 percent of the world's data had been created in just the past two years
- Facebook alone collects more than 500 terabytes of information every day
- Predicted rates of growth vary, but it appears the data boom is still in its beginning stages

Data alone presents a few problems, but many of them emerge from a single misguided view – that big data *is* the answer, not *part* of the answer.

“Complete context” is drawn from tracking how a business is being targeted, who/what group is behind the attack, what the attackers are after, what they make off with each time, and how the competition is faring.

It's not just about shoveling more data into the big-data pile; it's about using the surrounding information, which initially may not seem relevant, in order to provide a more accurate, personalized data set. It’s a process that involves looking closely at the impact on employees, customers, suppliers and technology infrastructure. It's having data about the target business itself: its operations, assets, software and hardware in use, and more.

In short, it's having a baseline of good data from a variety of angles that is rounded out with this idea of "complete context" – and then viewing all of that through the lens of the specific organization and its key business areas in order to get smart and useful information.

Data without “complete context” is like a box of chocolates without the filling. It looks tasty, but bite into any of it and its nothing but air. All the good stuff is missing.

Data Doesn’t Replace Analysts; It Empowers Them

Data is excellent for finding correlations, but is difficult for drawing conclusions. Understanding the “why” is often the most important question, and data analysts are needed to fill that gap. Data analysts using straightforward cybercrime data provides the best of both worlds.

In analyzing cybercrime, for example, distributed denial-of-service attacks may have

Why Less is More when it Comes to “Big Data” Threat Intelligence

Business’ are drowning in data, wasting precious man hours and budget resources trying to sort through the troves of information for what’s relevant to their organization. How do you know what’s useful? Forrester Research analyst Rick Holland said it best in a recent blog titled: “If everything is threat intelligence then nothing is threat intelligence.”

A comprehensive database is certainly an important aspect when it comes to threat intelligence, but without some key attributes that lead to real actionable intelligence, organizations can be left floundering.

Big Data Cyber Intel Should be...

- **Comprehensive**: Data needs to be collected into a model that paints a full picture and is easily distilled into useful intelligence – to help protect an organization’s assets immediately
- **Accurate**: Data needs to be correct; any potential fault or bias in the data sources should be disclosed up front
- **Relevant**: Data must be applicable to the organization using it; therefore, it must be easily integrated and flexible; information pertaining to the financial sector is likely useless for those in energy
- **Timely**: Data must be current and reflect up-to-date threats and solutions; older data has value, but it should be honest in what it is
- **Tailored**: Data should be tailored towards a specific purpose; if it’s not adding to that purpose, it’s unnecessary and is only muddying the water

risen sharply in the retail sector or hijacked Twitter accounts may have dropped 30 percent overall, but what good is that data? Without context, it's empty; no action can be taken.

However, knowing those DDoS attacks are likely tied to the recent batch of low-level extortion attempts or that the drop-off in Twitter hijacking occurred over the same period that Twitter rolled out two-factor authentication takes that abstract data and gives it real-world, practical implications.

Data Shouldn't Create a Maze to Get Lost In; It Should Create a Guide to Follow

The problem with having too much information: it's easy to get lost in the details.

This applies even more to cybercrime data, which because of its nature can be full of very specific technical details. A paragraph or two on packets or malware signatures or command and control servers is enough to send 95 percent of the population (and most business executives) running. And for good reason.

Most CEOs and most small business owners don't care about the in-depth technical details behind an attack. From a risk intelligence point of view, it's rather useless. They want to know two things to take action:

1. What do we need to protect
2. What's the best approach to protect these assets

To really answer these questions, organizations need a high-level view of their cyber risks. Unfortunately, it's all too easy to get caught staring down the barrel of a microscope at the massive amount of low-level noise.

For example, tracking the small changes in a piece of ransom-ware provides little value to most businesses. What matters is simply knowing that ransom-ware is on the rise, that it can take over computers and lock their files, that traditional antivirus isn't stopping it – and, most importantly, how to defend against it. The rest, for most, is just noise.

Data Isn't One-Size-Fits-All; It Must be Tailored

Every business is unique. Data needs to be able to adapt to that reality, or it's not useful.

The biggest cybercrime story of 2013 was the Target data breach, which exposed payment card information on 40 million consumers and the personal details of up to 70 million more. Troves of information now exists on that breach: what happened, how it happened, the impact it had in the media, the impact it had financially, and the impact on potential regulation. But if a business doesn't perform point-of-sale transactions, most of that information falls straight into the "it-doesn't-affect-me" category.

However, pieces of that story may be beneficial to a business. For example, the fact that the origin of the Target breach was through a third-party vendor may highlight potential weaknesses in another company's supply chain.

Many variables come into play when it comes to what concerns a business may have and what they need help protecting against: the industry sector, any infrastructure they have, the size of the company, the size of the supply chain, their location, and their online presence just to name a few.

With so many potential variables at play, it's important that data has the flexibility to match the needs of a business.

Not All Data Created is Equal; It Needs to be Both Relevant and Useful

It's true; less is often more. That goes against the "big" of "big data," but it's crucial. In the race to be the biggest and baddest, it's easy to muddy the waters with data that doesn't fit your objective.

Data should be relevant to its purpose. The structure of the data, what's collected, and, equally important, what's not, all are based around that purpose. For cybercrime, the purpose is simple: presenting the confusing and often technical world in a clear and straightforward manner. It's about a shift in approach to a high-level, easy actionable view that everyone can easily understand regardless of their technical expertise.

And that's because, behind it all, data needs to be useful to its audience. There are a ton of operations furiously collecting and combing through huge bins of packet data and terabytes of log files, and they serve their purpose. But focusing too much at that level can be a disservice to large sections of a potential audience: the people that want to simply know what they're getting hit with, how threats are occurring and what's happening as a result.

Staying Safe with Intelligent Security Analytics

When it comes to presenting cybercrime through the lens of big data, SurfWatch Analytics was created on that foundation of "complete context," essentially, empowering analysts with relevant, useful and tailored data that provides a simple, straightforward guide through the world of cybersecurity and cybercrime.

The problem with cybersecurity – just ask anyone – is that it can be quite complex. It's technical. It's always changing. There's a steep learning curve. Traditional security practices and approaches are reactive in nature because of this. On top of that, there's an immense amount of data that can be collected. It can be overwhelming. That's why it's so important have a good method of organizing all of that complexity into a usable information model that allows an analyst to quickly act on and make their business safer.

When it comes to security and threat data, what's really important in understanding an organization's true risk and the potential impact on the business?

Risk Intelligence that answers who (Actor) did what to whom (Target), what happened (Effect), and how did they do it (Practice) provides the method of normalizing all of the data that is out there and making is consumable.

Taking that complex world and organizing it into what matters helps an organization answer these important questions: what are the top practices associated with fraud in financials, what effects are trending upwards in healthcare, which type of organizations are being targeted in entertainment, what threats are similar companies in facing?

Turning a Stream of Data into CyberFacts and CyberInsights

At the core of SurfWatch Analytics are CyberFacts and CyberInsights, which translate volumes of cyber-related information into useful intelligence that organizations can quickly and easily understand and act on.

What is a CyberFact?

A CyberFact is raw cyber data composed of an Actor, Target, Effect, and Practice. The SurfWatch Analytics engine continuously collects cyber-related information from a wide range of structured and unstructured sources – from social media, news and blog data feeds, security vendors, vulnerability data feeds and more – and normalizes this information into CyberFacts so they can be processed and analyzed to derive CyberInsights.

What is a CyberInsight?

CyberInsights are CyberFacts that have been analyzed by a combination of proprietary cyber risk analytics, Natural Language Processing and human intelligence. CyberInsights answer the most critical cybersecurity questions such as "What should my business worry about most?"

With this model and format, security is easily understood by the business and most importantly what the impact to the business may be and how to get out in front of potential attacks.

SURFWATCH CYBER IN SIGHT

About SurfWatch Labs

SurfWatch Labs delivers cyber risk intelligence solutions that help organizations understand the potential for cyber-attacks, determine the impact to their business and proactively address threats head on.

SurfWatch Labs was formed in 2013 by former US Government intelligence analysts to go beyond the low-level threat intelligence approach that can drown organizations in data. By aggregating and automatically analyzing vast amounts of data from a wide range of structured and unstructured sources, SurfWatch enables organizations to zero in on their unique cyber risk profile and ensure the most effective risk management strategies are identified and implemented.

With SurfWatch, organizations can immediately understand and act on their cyber risk. SurfWatch Labs: Cyber In Sight. For more information, visit www.surfwatchlabs.com.

Contact us at:

info@surfwatchlabs.com

(866) 855-5444

Follow us at: