CYBERSPRINT
BREAKTHROUGH SECURITY

EDITORIAL

WHY YOUR BRAND DNA IS THE FOUNDATION OF YOUR SECURITY POSTURE

BY **WILLEM VAN ZWIETEN**
LEAD DATA SCIENCE & ANALYTICS

WHY YOUR BRAND DNA IS THE FOUNDATION OF YOUR SECURITY POSTURE

BY **WILLEM VAN ZWIETEN**
LEAD DATA SCIENCE & ANALYTICS

The internet is huge and is expanding every day. While this has many positives for businesses, managing the potential risks in this environment can be daunting. The reality is that across the internet brands are susceptible to everything from brand abuse to phishing websites. So, how is it possible that organisations can keep track of the web-based assets that belong to them, and at the same time distinguish them from something that may only look like it's theirs?

Finding and verifying all of a company's web assets across the entire internet is a massive undertaking. You essentially need to filter the whole internet and try to pick out what is relevant, and then set about detecting the risks — or even potential risks — within what you have found.

This isn't a process that can be managed manually. The staff-hours alone would make this hugely prohibitive, and that's without taking into account the potential margin for error. Instead, it requires a different approach, one based around automation.

At Cybersprint, my team and I work on exactly those kind of solutions. We've developed our own algorithms to define what distinguishes a client's brand-owned site from everything else on the internet. We refer to that as a company's Brand DNA. These special characteristics help us to predict and identify where any brand-related assets are across the entire internet, and how they should be investigated further.

The concept of an organisation's Brand DNA breaks down into two areas: what is unique by design and what is unique by comparison.

> THE CONCEPT OF AN ORGANISATION'S BRAND DNA BREAKS DOWN INTO TWO AREAS:
> 1. WHAT IS UNIQUE BY DESIGN
> 2. WHAT IS UNIQUE BY COMPARISON.

UNIQUE BY DESIGN

All brands have different design elements that help set them apart from other brands. This can be everything from their name and logo, to the different fonts and colours they use in all their communications and websites. By ingesting this data into our algorithms we are able to scan the internet for any web-based assets that may be relevant to a company, based on these key brand elements.

While the elements of 'unique by design' are relatively easily understandable by humans, no organisations want to have their time taken up manually searching through millions of images every day in order to help them locate the web properties that might belong to their organisation.

UNIQUE BY COMPARISON

Conversely, 'unique by comparison' focusses more on the elements that a human would probably not be able to figure out by themselves. As we suggest potential new domains to customers, we build up a pool of assets. Automation allows us to find patterns in these assets that might not be immediately obvious to humans, such as elements of metadata, nameserver details, or even where a website is hosted.

Although unique by design is more about what you actually see on a website and unique by comparison focuses on the back-end, in reality there are overlaps and the two things feed into each other.

As a very basic example: if a domain is hosted on name-server where other company assets are hosted, AND the company logo is on the page, then the chances are this domain is a company-owned asset. In effect, the two approaches strengthen each other. By analysing all these details together, our algorithms can increasingly accurately score how likely an asset is to be owned by a company. I should add here that unique by comparison is based on comparing a lot of features at once, so it is often not as clear cut as the above example.

COMBINING HUMANS AND AI

Ultimately, automating the process in this way helps to create a minimal-touch process for companies. The algorithms do all the filtering, enabling the creation of a much-reduced list of assets for the company to look through. Basically, we're able to break down that list to a very small percentage of the internet that they actually need to look at and then analyse the risk those assets pose to the organisation.

ULTIMATELY, AUTOMATING THE PROCESS IN THIS WAY HELPS TO CREATE A MINIMAL-TOUCH PROCESS FOR COMPANIES.

We also use something which we internally label "AI²" (artificial intelligence with analyst interaction). This essentially means we're adding a human layer to the automated process, for both input and output checks. While the algorithms do all the heavy lifting and aid scalability, the human element allows us to finetune or dive deeper into certain automated findings.

DETECTING MALICIOUS ASSETS

While the algorithms are principally focused on establishing a brand's attack surface, a useful by-product is that they can also locate malicious assets, such as potential phishing sites. For example, if something looks like it belongs to the customer, but doesn't **actually** belong inside their direct digital infrastructure, then clearly there is an increased likelihood that it is either a brand abuse or phishing site.

On top of this, as part of our search process we can also automatically create combinations of possible URLs that cover common search errors such as typos or “fat finger” errors within brand names, and then hunt for those — clearly the likelihood of these URLs being rogue sites is greatly enhanced.

THE CLEAREST VIEW OF YOUR ATTACK SURFACE

By combining all these elements, companies are able to get the most complete view of their potential attack surface. And with the use of enhanced automation techniques they can do so with minimum effort.

From this position companies are able to easily and quickly home in on the genuine items, and the areas that pose them the most risk. They can then use the resulting list to form the foundations from which they can apply the rest of their security strategy.

Interested to see how this works?
Visit our page below to read our detailed page on Vulnerability & Risk Assessment.

cybersprint.com/solutions/vulnerability-risk

ABOUT THE AUTHOR

WILLEM VAN ZWIETEN is the Lead Data Science & Analytics at Cybersprint. He and his team develop machine learning algorithms that fuel Cybersprint’s advanced Attack Surface Management platform.

Years ago, after spending a decade in Telecoms, Willem decided to contribute his Data Science skills to making the world a safer place through Cybersecurity.

In the vast world of cyber, Willem finds great satisfaction in uncovering what cannot be perceived by the human eye and accomplishing what cannot be achieved by the human hand.

ABOUT CYBERSPRINT

Cybersprint maps the attack surface of organisations and brands. We offer full visibility using continuous and automated digital asset discovery. Our zero-scope approach provides an outside-in perspective, eliminating blind spots.

Assets are individually scanned for a multitude of risk types. These insights empower cybersecurity professionals to prioritise the mitigation of vulnerabilities. Our integrated AI correlates dozens of data sources and uses a multitude of scanners, making risk relevant.

Cybersprint's SaaS platform allows organisations to manage and monitor risks with customisable filters and alerts, integrated into existing processes. Detect and prevent threats such as phishing, brand abuse, data theft and more.

Visit www.cybersprint.com