

Andrey Nikitin  
ENC 3252  
Oct 3, 2025

## Part 1: Synopsis

### Product/Service

The service being advertised is the cybersecurity tool BlindSpot. This is a tool that helps a company improve their defenses by simulating well-known attacks on their machines. You just download the executable on your endpoint, run it, and then use the web interface to control what happens next. They have 100s of attack campaigns containing infamous exploits to simulate. BlindSpot integrates with common defense tools like Defender and will automatically know whether the security tools logged the threat, detected it in an alert, or remediated it instantly. These statistics are saved so that the defenders can track their progress.

It is important to note that BlindSpot is a service, since it brands itself as a SaaS (Software as a Service), and thus companies pay an annual fee for a license to use the tool.

### Organization

The sponsoring organization is OnDefend, a penetration testing company founded in 2016 in Jacksonville Florida. In other words, other companies hire OnDefend to assess their security by hacking into their network. OnDefend has been rapidly expanding, increasing revenue by 114% this year and earning itself the title of 4th fastest growing company in the northeast. Unexpectedly, OnDefend has recently been part of some major events, like TikTok's security audit. Additionally, OnDefend

### Publishing Site

The publishing site of this native ad is Darknet Diaries, a cybersecurity podcast where the host, Jack Rhysider, adopts the style of an investigative journalist and interviews prominent hackers about their activities. This could be infamous criminals, former nation-state (government) cybersecurity specialists, or any hacker that got famous because of something they discovered or made. The podcast began in 2017, and has been growing ever since. In 2024, Jack Rhysider won the Ambies Award for [Best Knowledge, Science or Tech Podcast](#), which goes to show that it is the most popular podcast among the cybersecurity community. It is important to note that this podcast is largely a 1-man effort and Jack handles most aspects of it.

## Target Market

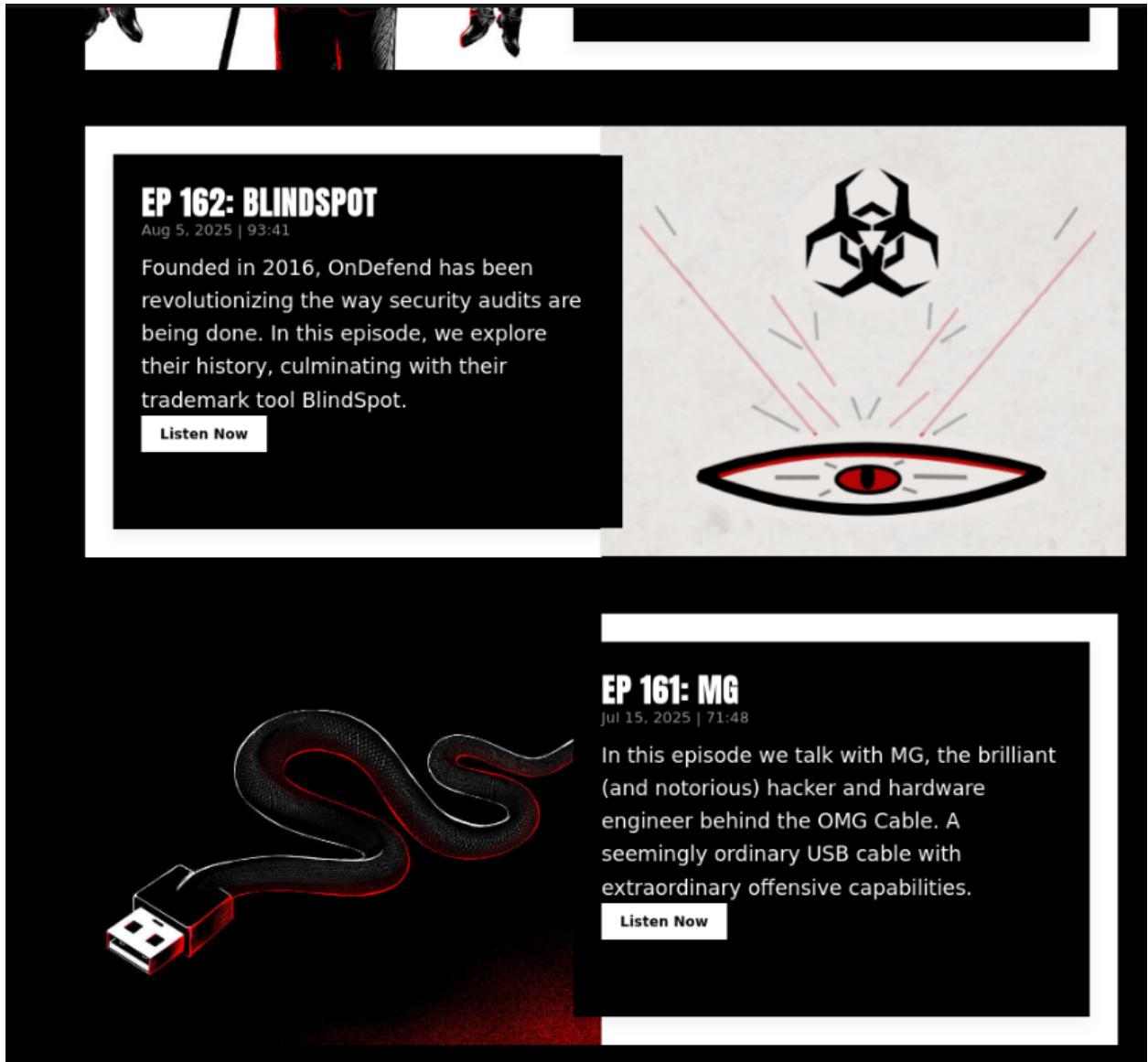
The target market for this platform is anyone interested in cybersecurity, as it is the most popular cybersecurity podcast. Jack explains technical concepts in simple ways, and focuses on the storytelling aspect of the hacks, making his content appealing to everyone from teenagers just getting started, to corporate CISOs. While [general viewership statistics](#) are available, there is no information on the demographics of Jack's audience.

## Design Documentation

In addition to being available on every major podcast platform, Darknet Diaries has a youtube channel as well as their own website where every episode is uploaded. Everything about the website, from the black, red, and white color scheme of the website, to the ominous electronic music used in episodes, plays into this gritty hacker culture. Visiting the main webpage will display the most recent as well as the most popular episodes as a list. In the menu bar, you can click on "Episodes" to view the full list. Each episode takes up a row on the page, encased in a rectangular white box consisting of two halves. On one half, lies a smaller rectangular black box, holding the Episode name and short description written in white text. On the other side lies the image for the episode. The detailed image reflects the topic of the episode, and is painted with only the colors red, black, and white, often displaying mysterious or threatening themes. Clicking on the white "Listen Now" button brings you to the episode page, which contains a play bar at the top to listen to the episode, followed by the conceptual art, short description, Sponsors section, Sources, Attribution, Equipment, and full length transcript. There is no indication of whether an episode is sponsored, other than the Sponsors section and ad breaks during the episode. In other words, the advertisements on Darknet Diaries are not native ads. Instead they interrupt the story with a louder, and more upbeat sponsored segment spoken by the host.

## **Part 2: Sponsored Content/Native Advertising Piece**

### Mock-up of Design



This is what the episode (BlindSpot) would look like on the Episodes page. To match with the theming of the rest of the webpage, there is no indication that the episode is sponsored until you click on that episode's page and see the "Sponsors" credit OnDefend.

## Content

[START OF RECORDING]

Jack (Narrating):

Hey, it's Jack, host of the show. Back when I was a network security engineer, one of my main jobs was setting up defenses — intrusion detection systems, firewalls, endpoint protection, all of it.

And after spending weeks or months tuning these tools, I'd sit back and wonder: "Are these things really working? If an attacker came through right now, would I even see it?" Because here's the truth—installing the tool is the easy part. Testing it? That's where it gets messy. You can configure rules all day long, but if you never check to see whether your defenses can actually catch real-world attacks, you're just hoping. And hope isn't a strategy.

(INTRO): [INTRO MUSIC] These are true stories from the dark side of the internet. I'm Jack Rhysider. This is Darknet Diaries. [INTRO MUSIC ENDS]

Billy:

Hey Jack, it's great to finally talk to the legend. Congrats on the Ambies award! You deserves it.

Jack:

Haha, legend? Many people have called me that, but the real legends are the ones who come on this show, like you. I still can't believe your company increased revenue by 114% this year. That's insane! Why don't you start by telling us about yourself?

Billy:

Thank you, Jack. So, my name is Billy Steeghs and I'm the COO of the penetration testing firm OnDefend. Founded in 2016 we've quickly risen to top with the release of our BAS SaaS, BlindSpot.

Jack (Narrating):

Woah. Okay, that was a lot of hacker lingo, so let's break it down. Traditionally, in cybersecurity, there are two main teams: the blue team and the red team. The blue team focuses on securing a company's network. They play defense, patching their systems and setting up tools that collect logs and alert whenever there is suspicious activity. Then, there's the red team, which focuses on attacking the network. This is what a penetration testing firm does. Their red teamers get paid by another company to hack into that company. How cool is that? Their goal is to identify all the vulnerabilities in their target while assessing how well the blue team defends against an active threat. This profession is known as penetration testing, since they penetrate into the company's network. While it seems like the two teams are antagonistic, in reality they go hand-in-hand, learning from each other as they improve in this constant battle of wits. But OnDefend does things a little differently... You may have heard Billy mention the

terms BAS and SaaS. BAS stands for Breach and Attack Simulation, which is similar to what a pentest is, and SaaS stands for Software as a Service. If you're not sure how these tie in to the story, don't worry, he'll explain later.

Jack:

That is quite the feat! I bet you encountered a lot of exciting scenarios along your path.

Billy:

Exciting is one way to put it (chuckles nervously). One of the most frightening experiences I've had was during a web application pentest for a medical company. They relied on a third-party vendor to generate all their PDFs linked to medical records. After some probing, I found the vendor's site and a version number that led me to a series of vulnerabilities (CVEs). Using this information, I developed a tool that could brute force random patient IDs, giving access to medical records.

When I presented my findings, the client dismissed it as an unlikely scenario, saying it would require insider access. Fast forward a few months, and the same company made the news—hundreds of medical forms were leaked due to the exact type of brute force attack I had warned them about. This was not a database leak but a targeted attack, and they paid the price for not taking the threat seriously.

Jack:

They dismissed your findings? That's tragic... why wouldn't a company want to patch all vulnerabilities that they have?

Billy:

Well there's a few reasons Jack. Security is expensive, and it takes time. Unfortunately, security is rarely a company's #1 priority. It doesn't bring in any profit and it's difficult to convince someone of the potential losses from a security breach unless they experience it first hand. As a result, a company's blue team is often understaffed and can only afford to patch the vulnerabilities with highest risk, a combination of severity and likelihood. For our client specifically, you run into additional issues from a hospital. Technology in healthcare needs to be functional at all times, or else lives will be lost. Plus, most of this technology is old, like decades old. It's a common practice for hospital devices to be completely isolated from the internet to minimize the attack surface, all the possible paths an attacker can get in. If your machine is less exposed, it's less likely to get hit. However, this also means that any updates need to be manually applied, which can take a long time.

Jack (Narrating):

He's right. Hospitals are extremely vulnerable, and since they contain such sensitive and lucrative information, they make juicy targets for attackers. Most of the time, hackers will avoid hospitals for ethical reasons, but not always. If you want to hear another example of a hospital being hacked, then you can listen to Darknet Diaries Ep. 14: #OpJustina

Billy:

There's one last reason. While it never occurred for us, a weird dynamic can develop between the blue and red team. They treat it like a competition, and whenever a pentest happens, the blue team feels like they lost. Instead of commending them for what they did right, the red team will gloat over the blue team and leave without suggesting how to improve their defenses. This is demoralizing for the blue team, and discourages them from patching vulnerabilities, or engaging in future pentests. I've seen it happen before. Target has stopped hiring outside pentesting contractors for this very reason. That's why we at OnDefend decided to take a different approach.

Jack:

Are you talking about BlindSpot?

Billy:

That's exactly what I'm talking about. Instead of relying on people to pentest a network, we decided to automate it. That's why it's a SaaS - Software as a Service. Instead of paying for a contractor to come and break into your network, companies are paying for a license to our tool.

Jack:

Okay... but how does this tool actually work?

Billy:

You just download the executable on your target endpoint, and then use the web interface to run an attack campaign. We have a library of 100s of different campaigns to choose from, built using the knowledge we've gained over the years in our red team engagements.

Jack:

That sounds simple; I can see why companies are buying into this model. But something you said earlier caught my attention. The blue team is getting demoralized during penetration tests? That's awful. How does a tool like BlindSpot change the situation?

Billy:

Well, with BlindSpot it's no longer a competition of red v blue. The blue teams are now running red team campaigns against themselves. To them, it just feels like they're testing the tools they've set up. Plus, in a traditional pen test it's usually a one-and-done thing. You hire the penetration testers, they give you a report, and then you don't hear from them again unless you pay for another penetration test. There is no reliable way to ensure the blue team is successfully responding to the identified threats. On the other hand, if the blue team has constant access to a tool like BlindSpot, they can retest their network each time they make a change. BlindSpot even integrates with common security tools like Defender and Sentinel One to automatically identify whether the blue team is detecting and responding to threats, and tracking their score so that they can see their progress over time. It's not the traditional way of doing things, but it works. In fact, it works so well that we were asked to do the security audit for TikTok.

Jack:

Wait, hold up. TikTok? That's huge. What was that like?

Billy:

Yeah, it was a big deal. We can't go into too many details, but it was validating to see that the same tool we designed for smaller companies could scale to a global giant like TikTok.

Jack (Narrating):

That's right, no matter how big you are, every company has blind spots in their security. Thank you for helping them find it and coming here to tell your story. It's an important one. Attackers only need one blind spot to get in. But if you keep testing, if you shine light into every corner, you reduce those blind spots one by one. And that could make the difference between a headline breach... or nothing at all.

(OUTRO): [OUTRO MUSIC] A big thank you to Billy Steeghs for sharing this story with us and to OnDefend for sponsoring this episode. Did you enjoy not having any ad breaks? You can find a link to their tool, BlindSpot, in the show notes. This episode was created by me, the bit-bumbler, Jack rhysider. Our editor is the silicon sorcerer, Tristan Ledger. Mixing is done by Proximity Sound, and our interim music is done by the mysterious Breakmaster Cylinder. One time I went into a client's data center to do some work on their servers, and I found a computer that was so old, its IP address was 1. Just the number 1. This is Darknet Diaries.