




CASE STUDY  
**Education**

# Cybersixgill is a force multiplier for client under pressure

## At a glance

---

 10k+ employees

 Education

## Overall benefit

---

*Analysts improve their ability to collect threat information while significantly reducing their workload*

## The Challenge

As the only analyst in the organization for a number of years, this client was battling to gain access to dark web sources and translate forums manually. "Before Cybersixgill, I would use open source tools and my own access to Dark Web forums. I would use GitHub tools and my own investigation on Dark Web forums, and it would take an enormous amount of time," comments the client. Looking to save time in their working week, the user turned to Cybersixgill for assistance.

## The Solution

Using Cybersixgill's Threat Intelligence Portal, the client was instantly able to access sources they had not seen anywhere else, including closed access forums and marketplaces. "We're leveraging it to provide value to the incident response team, to the governance and compliance team, to the access management team and to the vulnerability assessment team. We're leveraging it for a lot. As for expanding our usage of it, we're planning on trying to find ways to automate some of the inter-group alerting and use of the tool," says the client.

## The Results

Upon reviewing Cybersixgill's Investigative Portal, the client says "The size and scope of the solution's collection are pretty impressive. I am impressed with the ease through which the tool allows you to track threat actors who are likely to target you, on a variety of underground forums which are closed. These are sources that would require a solid effort to infiltrate. The automatic translation of any exchange within the platform makes it the most expedient solution for automated threat intelligence and chatter monitoring.

It is also of the highest importance that it runs on a collection of deep web, dark web and closed sources. This tool is a must for any organization that has a large footprint. The solution's approach of using limited

open source intelligence and focusing, instead, on the Deep Web and Dark Web is what seals the deal. That is why I like them. They are not just aggregating open source news and feeds, they're actually gaining access to real intelligence.

For me, personally, and the organization, there has been immense benefit because it has given me early detection of imminent attacks, but not just against my organization. We have also been able to help other organizations, based on the attacks that are being launched against our vertical, meaning companies and organizations that fit our profile.

It also enables us to do advanced analysis, such as threat-actor profiling. Being able to do advanced threat-actor network analysis allows us to take a higher view of an imminent attack and possible exploitation of vulnerabilities. That's helpful because it informs us about what's about to be exploited—what these criminals are looking for, what the threat-actor might be exploiting against the vertical itself.

I've seen an incredible return on the investment, in the form of time-savings and extremely valuable alerting on infrastructure attacks against us, alerts that I would not have seen if it wasn't for them.

I have been very vocal about how much this tool has helped. I'm a big proponent of it. When I talk to people and collaborate with people in other organizations and they say, 'Oh my God, how did you know that?' I'll tell them I knew because of this tool. For example, by setting queries to track exfiltration of ransomware gangs that employed the double ransom technique, it can exfiltrate the names of any companies that are being ransomed, before they hit the news. That allows me to cross-reference with our third parties and to tell my CSO that a third party is being compromised. I can tell him that before it even hits the news, and that we need to go into protection mode and assume that there might be potential impact to our organization, based on their compromise and the exfiltration of that data."

## About The Investigative Portal

Combining unparalleled threat data collection capabilities with limitless search functionality and automation, the Cybersixgill SaaS Investigative Portal delivers contextual visibility into the clear, deep and dark web. With secure, covert access to our complete body of collected intelligence, your team can proactively prioritize and respond to threats that are targeting your critical assets, prevent fraud, data breaches and investigate threats in real-time to minimize your attack surface.

**[Learn more](#) about our threat intelligence Portal and how it can support your ongoing cyber security activities.**

[Explore the Investigative Portal >](#)



---

**[Book a Demo](#)**

---

**[Visit Cybersixgill](#)**

---

Follow us

