Making Cyber Investigations Significantly Faster and More Thorough

CyberProof®
A UST Global Company

EXECUTIVE SUMMARY

CyberProof is a global managed security service provider (MSSP), with team members on multiple continents working with clients including major enterprises. Understanding the threat intelligence value of the deep and dark web, the company's cyber threat analysts routinely gather and investigate intelligence from these dark sources. Until the company started using the Cybersixgill Investigative Portal, this process required those analysts to invest significant time and resources in gaining access to dark sources.

By using the Cybersixgill Investigative Portal to gather relevant threat intelligence, CyberProof has replaced the painstaking process of gaining access to dark sources individually with a streamlined, convenient approach to searching for valuable information. As a result, CyberProof has dramatically accelerated the way it investigates possible threats and vulnerabilities. Meanwhile, the company has enhanced the comprehensiveness of its investigations by giving its analysts easy and convenient access to today's largest collection of threat intel from the deep and dark web.

KEY BENEFITS

RAPID INVESTIGATIONS

of cyber threats and vulnerabilities

COMPREHENSIVE COLLECTION

of threat intelligence

REAL-TIME ALERTS

of activity discovered on the deep and dark web

INTEL FROM THE DARK WEB

with no need for cumbersome process of gaining access

THE CHALLENGE

As a global managed security service provider offering a variety of cybersecurity services to major enterprises, CyberProof understood what a valuable and comprehensive source of threat intelligence the deep and dark web could be. Frequently, the collection and analysis of intel from these dark sources was a key part of the services that the company offered its clients. And CyberProof used this approach to gain important insights into what threat actors were up to, including in cases in which CyberProof's assistance was sought out by businesses that had fallen victim to cyberattacks. In these cases, CyberProof could use its intelligence to tell whether a given client's intellectual property had already been compromised and leaked on the dark web.

The problem was that this approach to gathering threat intelligence from the deep and dark web was cumbersome and time-consuming. Threat analysts often had to spend significant amounts of time seeking access to dark sources, using tools such as VPNs to avoid arousing suspicion. And even after CyberProof's analysts did gain access to channels on the deep and dark web, it was difficult to tell whether any given investigation's use of the dark web was sufficiently comprehensive. The vastness of the deep and dark web, combined with CyberProof's individual process of gathering and analyzing threat intel, meant that they could never fully rule out the possibility that one of their investigations had missed a relevant post on an underground forum.

> “Before we started working with Cybersixgill, in a typical investigation it would take approximately two working days for me to gather my initial findings... Today, to get my initial findings through Cybersixgill's platform takes me about one hour.”
>
> **Orel Pery**
> Head of Cyber Threat
> Intelligence, CyberProof

THE SOLUTION

To empower its cyber threat analysts to conduct investigations rapidly and comprehensively, CyberProof decided to start using the Cybersixgill Investigative Portal. This solution gives CyberProof's analysts convenient access to Cybersixgill's collection of threat intelligence gathered automatically from the deep and dark web – the largest such collection of any solution on the market.

When investigating a possible threat, CyberProof's analysts can easily search the Investigative Portal for relevant posts from dark sources. They also have the option of setting up automatic alerts based on specific parameters, so that they will be informed of any new intelligence as it becomes available. And, since all of the threat intel is stored locally on Cybersixgill's own servers, those analysts never need to worry that their searches could inadvertently tip off the threat actors they're trying to investigate.

THE RESULT

By using the Cybersixgill Investigative Portal instead of searching the deep and dark web directly for threat intelligence, CyberProof has dramatically accelerated its investigations of possible cyber threats and vulnerabilities. Whereas the company's analysts used to spend roughly two full workdays on the collection phase of a typical investigation, now this phase generally takes approximately one hour. And whereas new employees used to require about one to two weeks to prepare enough in order to start working productively, now new team members can typically jump right in and start conducting investigations after only two or three days on the job.

Meanwhile, working with Cybersixgill empowers CyberProof's threat analysts to conduct more thorough and reliable investigations. Not only do they have access to Cybersixgill's full collection of threat intel, but they can access it all through the Investigative Portal's intuitive interface. And, with this intel analyzed and classified automatically by Cybersixgill's AI-powered engine, they can quickly and conveniently find the most relevant threat intel for any given investigation. In fact, CyberProof's team members often make a point of letting prospective clients know that they work with Cybersixgill, understanding that the comprehensiveness that Cybersixgill's technology adds to their investigations is a major benefit for clients.