BITSIGHT

EBOOK

Seven Strategies for Researching the Deep and Dark Web

Table of Contents

01

Introduction

01 Introduction

The deep and dark web is a treasure-trove of information on threat actor activity, however making use of this resource to protect your organization can be (to the uninitiated), challenging. In this guide, we discuss the 7 strategies for researching the deep and dark web, as used by Bitsight analysts, to help enhance your threat intelligence program.

02

Getting Started

02 Getting Started

Creating a complete intelligence picture of the threat landscape relevant to your company or organization is a complex and difficult task. First, you must begin with a question. Intelligence questions based on the deep and dark web broadly fit into the following categories:

- Who may be conducting or preparing to conduct a certain type of cyberattack?
- What are threat actors targeting?
- How are these threat actors aiming to strike/which TTPs are they using?
- How much (to what extent) is this threat materializing?

After forming the question (or questions) that will drive an investigation, an analyst must define a methodology and framework to answer it. While each scenario is different, there are some generally promising ways for analysts to confirm or refute a hypothesis.

Depending on the nature of your threat investigation, your best approach may be to combine several strategies in order to broaden your search. Below you'll find the seven strategies that we at Bitsight have found to be especially useful.

The 7 Strategies for researching the deep and dark web

01 Aggregate mentions to determine a trend

02 Follow major events and correlate to dark web activity

03 Follow the services

04 Search for tools in the attack chain

05 Search for products of attacks

06 Search for indirect indications

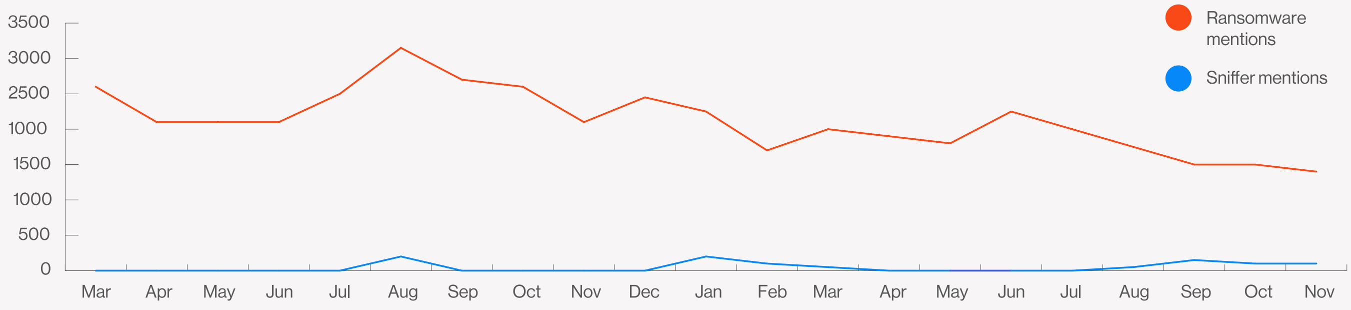
07 Extrapolate what threat actors aren't saying

Strategy 1: Aggregate mentions to determine a trend

By tracking the number of query hits on your vendors threat intelligence portal over time, you can understand how the subject matter has been trending on the underground. Doing so can lead to valuable insights on how and when a particular phenomenon strengthens or diminishes.

In Bitsight's Investigative Portal, you can form a query to investigate anything on the deep and dark web—such as a threat type, specific actor, site, or general topic.

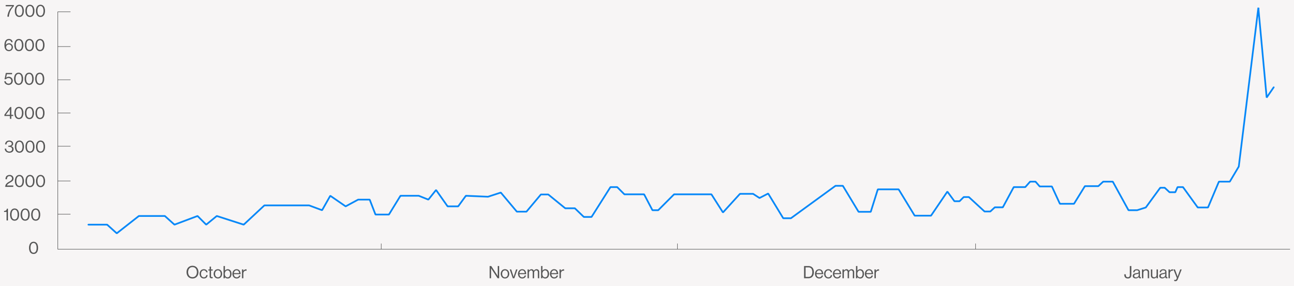
We can use this type of analysis to compare two trends. For example, both ransomware and credit card sniffers (such as those used by the Magecart group) accounted for very high-profile attacks in 2019-2020. However, when mentions of each one are compared (see graph below) we can see that ransomware is significantly more popular than credit card sniffers among underground actors. This can lead to additional insights about why this may be the case, for example, it may be that sniffing attacks are harder to execute or harder to monetize, and therefore attract less attention on the underground.



Numbers of monthly mentions of sniffers and ransomware identified on the deep and dark web in 2019 and 2020

A more advanced version of this approach is to look at the number of unique actors or sites involved in a particular query. This will show just how widespread and distributed a phenomenon is.

For example, the graph below shows that when "meme stocks" (such as GameStop) took off in January 2021, the number of unique actors participating in trading-themed messaging channels exploded as well. This highlighted that many new actors were joining the discussions.

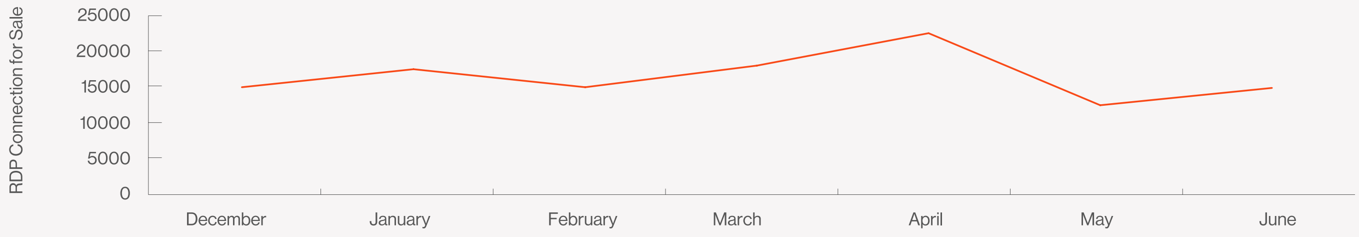


Numbers of unique daily users active on trading-themed messaging channels in late 2019 and early 2020

Strategy 2: Follow major events and correlate to dark web activity

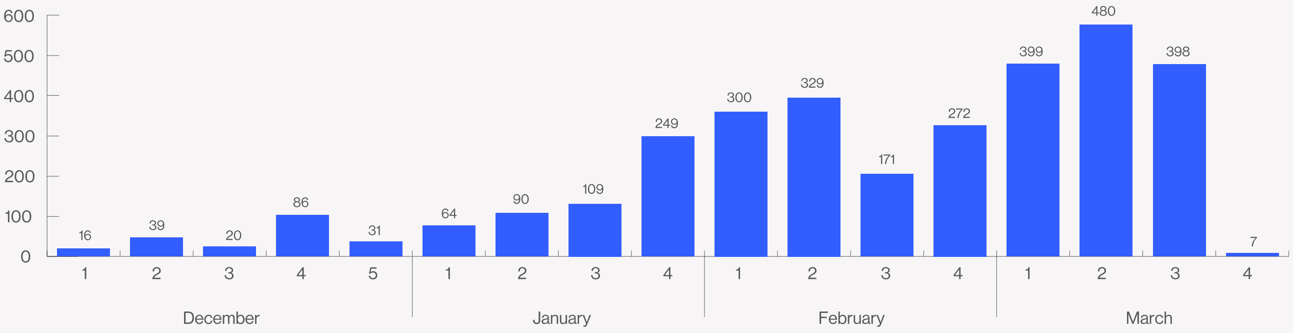
Major news stories, particularly involving cybersecurity and fraud, are often discussed in underground forums. Meanwhile, dark web actors seek to turn these events into opportunities. For example, as COVID-19 led to an unprecedented increase in working from home, we wondered if this would lead to an increase in RDP servers for sale on the dark web. When we searched the Bitsight Investigative Portal for mentions of RDP servers for sale during this period, our findings confirmed our hypothesis—that more remote working meant more compromised RDP servers.

Using the Bitsight Investigative Portal, analysts can access information on threat actor activity, including events in real-time.



The numbers of compromised RDP servers identified as being offered for sale on the dark web in late 2019 and early 2020

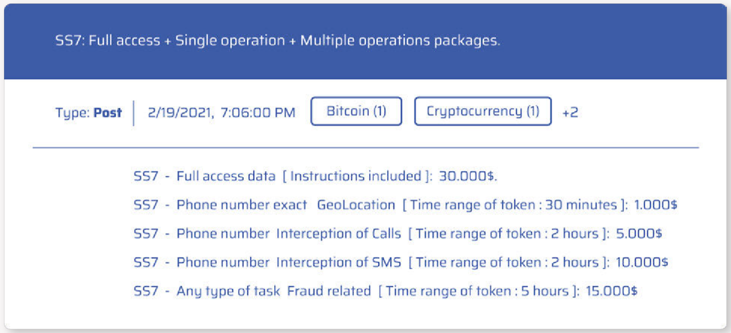
Similarly, as COVID vaccines were deployed, we found that the number of vaccines listed for sale per week on markets increased.



Strategy 3: Follow the services

Many dark web actors specialize in a particular field. Some are malware authors, some are social engineers and others know how to launder money undetected. On the underground, these actors offer their attacks as a service, enabling any aspiring attacker to assemble the necessary components in order to carry out a more sophisticated attack.

An analyst can investigate these elements to understand how widespread attacks are. Services that are rarer and demand significant fees, indicate that they are in high demand but difficult to perform. For example, this actor sells services intercepting mobile phone signals for fees ranging from $1,000 to $30,000.



SS7: Full access + Single operation + Multiple operations packages.

Type: **Post** | 2/19/2021, 7:06:00 PM

SS7 - Full access data [Instructions included]: 30.000$.

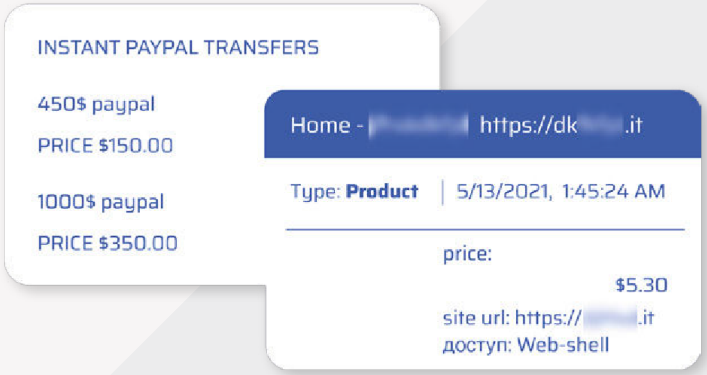
SS7 - Phone number exact GeoLocation [Time range of token : 30 minutes]: 1.000$

SS7 - Phone number Interception of Calls [Time range of token : 2 hours]: 5.000$

SS7 - Phone number Interception of SMS [Time range of token : 2 hours]: 10.000$

SS7 - Any type of task Fraud related [Time range of token : 5 hours]: 15.000$

Similarly, this actor offering PayPal "transfers" (i.e. money laundering) charges a 25% fee, indicating that these services are premium. Meanwhile, other services are inexpensive. For example, shell access to this compromised site, which can be used in a larger attack, is only $5.30. This indicates that website compromise is easier, more widespread, or both.



INSTANT PAYPAL TRANSFERS

450$ paypal

PRICE $150.00

1000$ paypal

PRICE $350.00

Home - [redacted] https://dk[redacted].it

Type: **Product** | 5/13/2021, 1:45:24 AM

price:

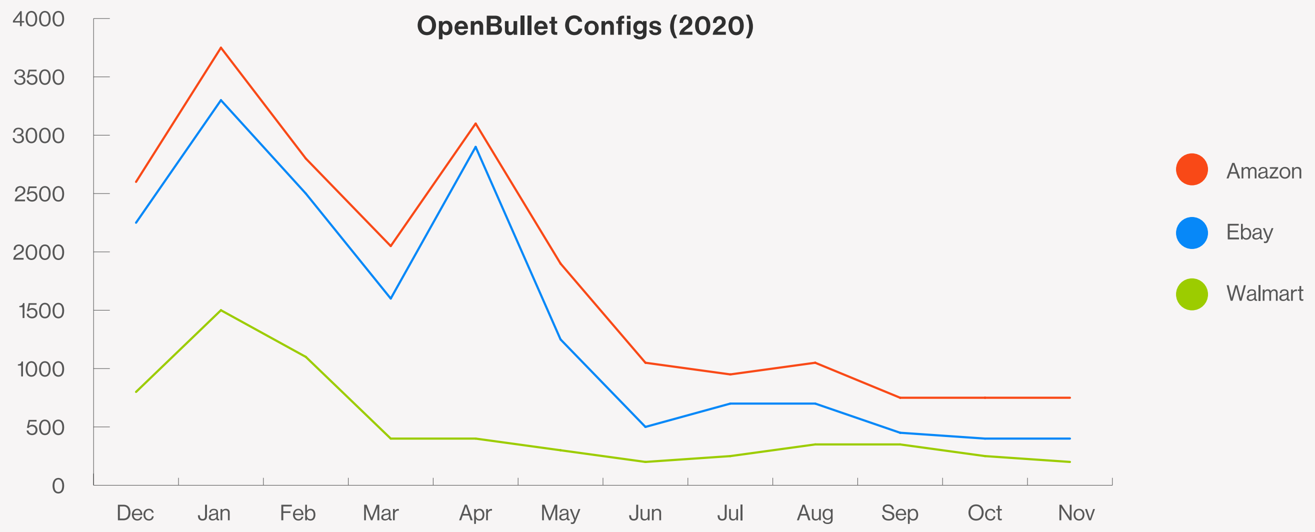
$5.30

site url: https://[redacted].it

доступ: Web-shell

Strategy 4: Search for tools in the attack chain

In an investigation focusing on TTPs, it is worthwhile to search for specific kinds of tools that could be used in a specific type of attack. For example, OpenBullet is a popular tool used in credential-stuffing attacks. By following the software's development, defenders can understand its capabilities and build protections. By investigating which services are most targeted by OpenBullet configurations, analysts can understand which services are most targeted in credential stuffing attacks.

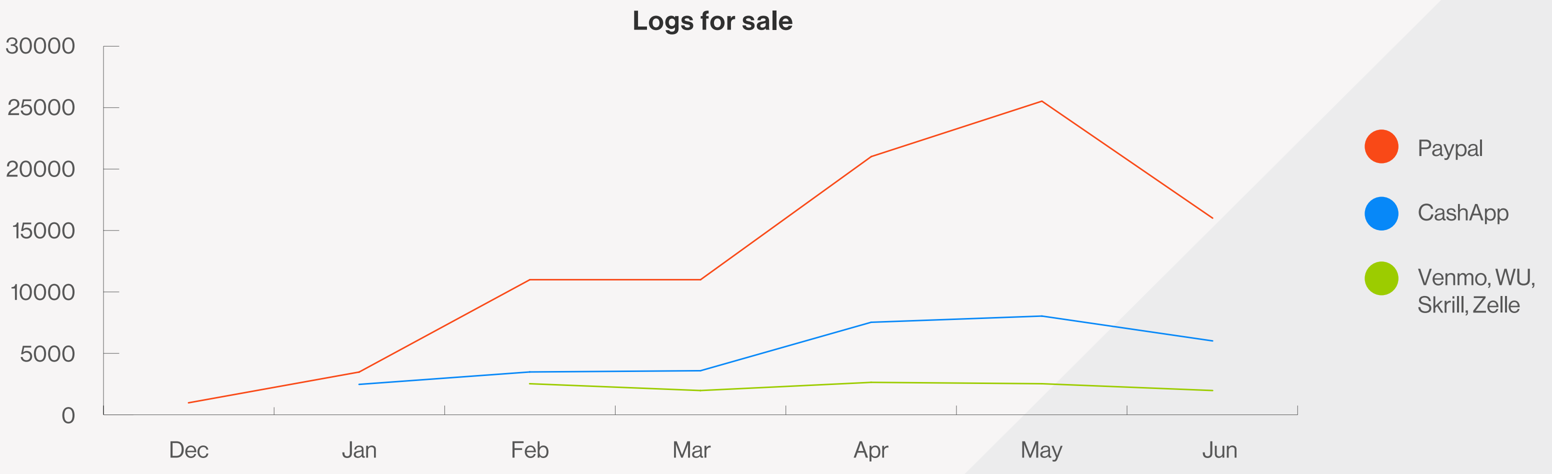


Monthly instances of leading eCommerce websites being targeted by OpenBullet configs in 2020

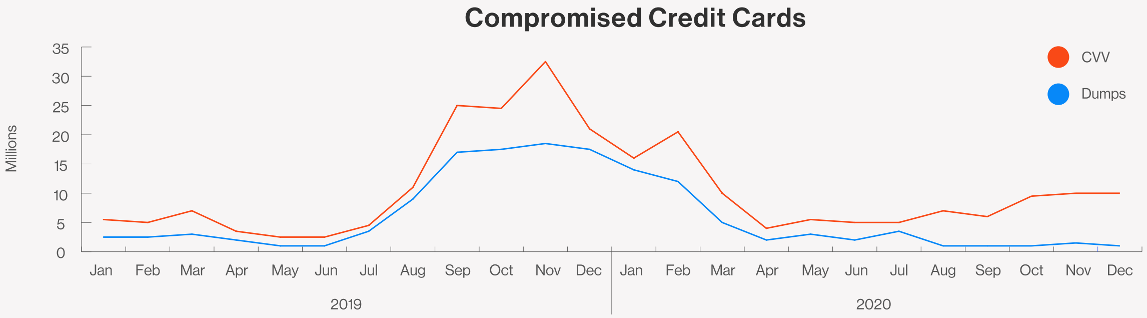
Using the Bitsight Investigative Portal gives users covert access to our complete, comprehensive body of threat intelligence to protect them against retaliation during an investigation.

Strategy 5: Search for products of attacks

While threat actors do not often reveal specifics about who or how they are going to attack, once they carry out a successful attack, they need to monetize it. Therefore, in dark web markets and forums, attackers sell compromised data, credentials and credit cards. Sometimes lower-value products are given away for free. Tracking products from attacks can indicate what may have been breached. For example, an increase of sold payment platform logs—valid usernames and passwords—of payment platforms indicates a major rise in phishing attacks.

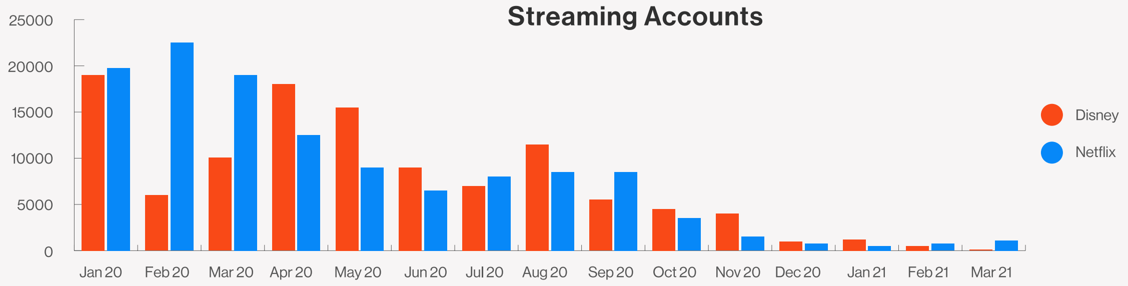


Similarly, following trends in quantities and prices of sold products can point to trends in this type of attack. For example, the chart below shows the quantity of compromised credit cards (in CVVs and dumps) sold in markets in 2019 and 2020.



Monthly number of compromised credit card credentials being sold in underground markets in 2019 and 2020

Finally, a sharp drop in the quantity of shared Netflix and Disney+ credentials may indicate that defensive measures are more effective at preventing credential stuffing.



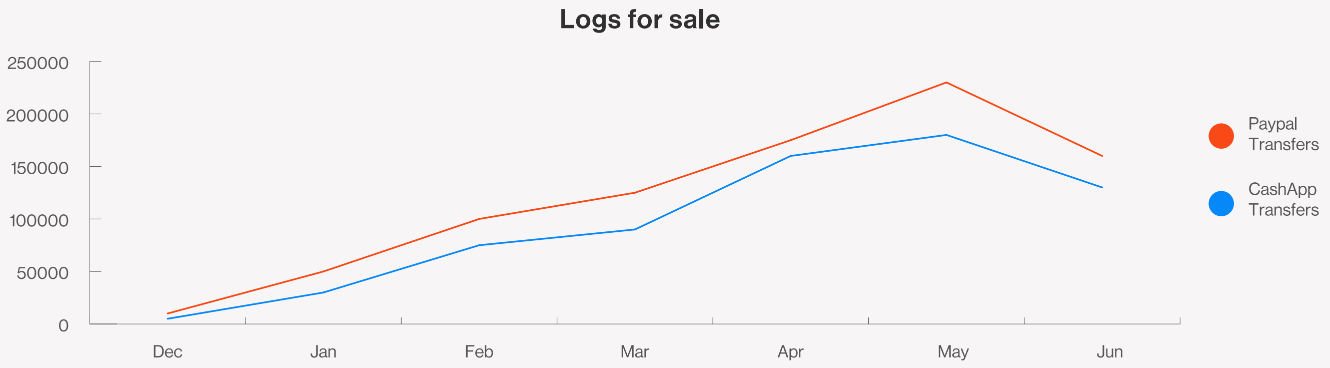
Monthly number of compromised credentials for streaming services being sold in underground markets in 2020 and early 2021

Strategy 6: Search for indirect indications

If an analyst cannot find hard proof confirming or refuting a hypothesis, it can be helpful to instead look for indirect evidence. If the hypothesis were true, what else would one expect to find (and vice versa)?

For example, we wanted to understand if there were indications of a rise in cybercrime during the COVID-19 lockdowns. We discovered that there was a massive increase in the number of mentions of transfer (money-laundering) services offered on PayPal and Cash App. While this does not directly prove a rise in cybercrime, we assessed that it was indicative of the general availability of fraudulently obtained funds.

Observing these numbers is like counting vultures around a lion's hunt: More prey brings more scavengers.



Some forums and marketplaces are closed to the majority of users and are therefore difficult to gain and maintain access. Bitsight's automated collection technology is undetected by limited access forums, giving users a unique insight into underground activity.

Strategy 7: Extrapolate what threat actors aren't saying

Although dark web actors for the most part do not share their plans, sometimes they tip their hand and reveal just a little too much. Perhaps they are unaware of, or apathetic to operational security. Or maybe they want people to know what they can do, as a proof-of-concept for more business, or bragging rights for more credibility.

Whatever the reason, if an analyst can find a "golden nugget," there's a good chance that many other actors are engaged in the same type of threat, but more discreetly.

For example, an actor posted that they were seeking a partner to help intercept mobilecommunication signals to capture SMS messages, then later wrote that they had "sourced it and got a working one." While we cannot tell from a single post to what extent this occurs, we can presume that many more actors are also engaged in this tactic.

03

Summary

03 Summary

Intelligence analysts live in a constant state of too much uncertainty, too much data, and a shortage of resources needed to process everything. After reading this guide, we hope that you now understand the environment that you are investigating, define the key threat intelligence questions to ask and form a way to answer these questions. By helping you identify the most relevant content from the deep and dark web, these strategies will empower you to investigate potential cyber threats comprehensively, accurately and efficiently.

It is important to remember that investigations are only as good as the tools you're using. Manual intelligence on the deep and dark web won't get you very far. You won't be able to access the right sites, perform mass keyword searches or extract any sort of quantitative insights.

Only with Bitsight's Investigative Portal can you efficiently discover the valuable, critical intelligence needed to keep your organization informed and secure.

About Bitsight

Bitsight is the world's leading provider of cyber risk intelligence, transforming how security leaders manage and mitigate risk. Leveraging the most comprehensive external data and analytics, Bitsight empowers organizations to make confident, data-backed decisions and equips security and compliance teams from over 3,200 organizations across 70+ countries with the tools to proactively detect exposures and take immediate action to protect their enterprises and supply chains.

Powered by the innovative BitsightIQ Platform, we deliver real-time threat insights uniquely tailored to an organization's external attack surface and third-party ecosystem.

For more information, visit Bitsight.com, read the Bitsight blog, or connect with us on LinkedIn.

sales@bitsight.com

BOSTON (HQ)
RALEIGH
NEW YORK
LISBON
SINGAPORE

Bitsight is a cyber risk management leader transforming how companies manage exposure, performance, and risk for themselves and their third parties. Companies rely on Bitsight to prioritize their cybersecurity investments, build greater trust within their ecosystem, and reduce their chances of financial loss. Built on over a decade of technological innovation, its integrated solutions deliver value across enterprise security performance, digital supply chains, cyber insurance, and data analysis.

BITSIGHT