cybersixgill

THE TOP 5 CYBER RISKS:

HOW TO PREVENT & PROTECT WITH THREAT INTELLIGENCE

TABLE OF CONTENTS

cybersixgill

FOREWORD

In 2020, the US cybersecurity market size was valued at USD 58.5 billion, taking the lion's share in a global market size of USD 167.13 billion*. The United States is also the most expensive country in regards to the average cost of a data breach - USD 8.64 million vs. the global average of USD 3.86 million*.

It's therefore no wonder that cybersecurity leaders are constantly in a race for better tools, knowledge, and methodologies to stay ahead of the threat curve. And as the cybersecurity industry continues to expand (expected to grow at a CAGR of over 12.9% between 2019 and 2026, reaching a whopping USD 13.9 billion*), professionals are quickly realizing the potential uses of threat intelligence and how it propels cybersecurity operations with its people, platforms, and processes.

The purpose of this eBook is to provide valuable insight into the top five cybersecurity risks, and how threat intelligence can help you detect and prevent them. More importantly, this overview is intended to help cybersecurity executives such as yourself determine what needs to be done in your own organization to maximize the efficiency of cybersecurity programs and the return on your security investment.

Brad LaPorte

Brad LaPorte,
Former Gartner Analyst & Cybersecurity Industry Expert

*source: https://www.mordorintelligence.com/industry-reports/threat-intelligence-market

INCIDENT MANAGEMENT

A RACE AGAINST TIME

When it comes to cybersecurity incident management, time is clearly of the essence. Cybercriminals are rapidly evolving, waging attacks of increasing sophistication, speed and scale. As attack velocity accelerates, the need for a well-functioning Security Operations Center (SOC) becomes ever more pertinent.

The SOC's primary function is to maximize an organization's overall security posture by reducing their potential risk exposure in the event of a malicious cyber-attack. Cybersecurity risks have the potential to affect all aspects and functions of an organization, threatening to inflict significant financial losses, disrupt business operations & availability, and damage brand reputation. As digital assets and attack surfaces rapidly expand, SOC teams face a tremendous challenge, overwhelmed by the growing slew of security alerts and data.

A SOC'S EFFECTIVENESS IN MINIMIZING CYBER-RISK EXPOSURE IS A FUNCTION OF 3 CAPABILITIES:

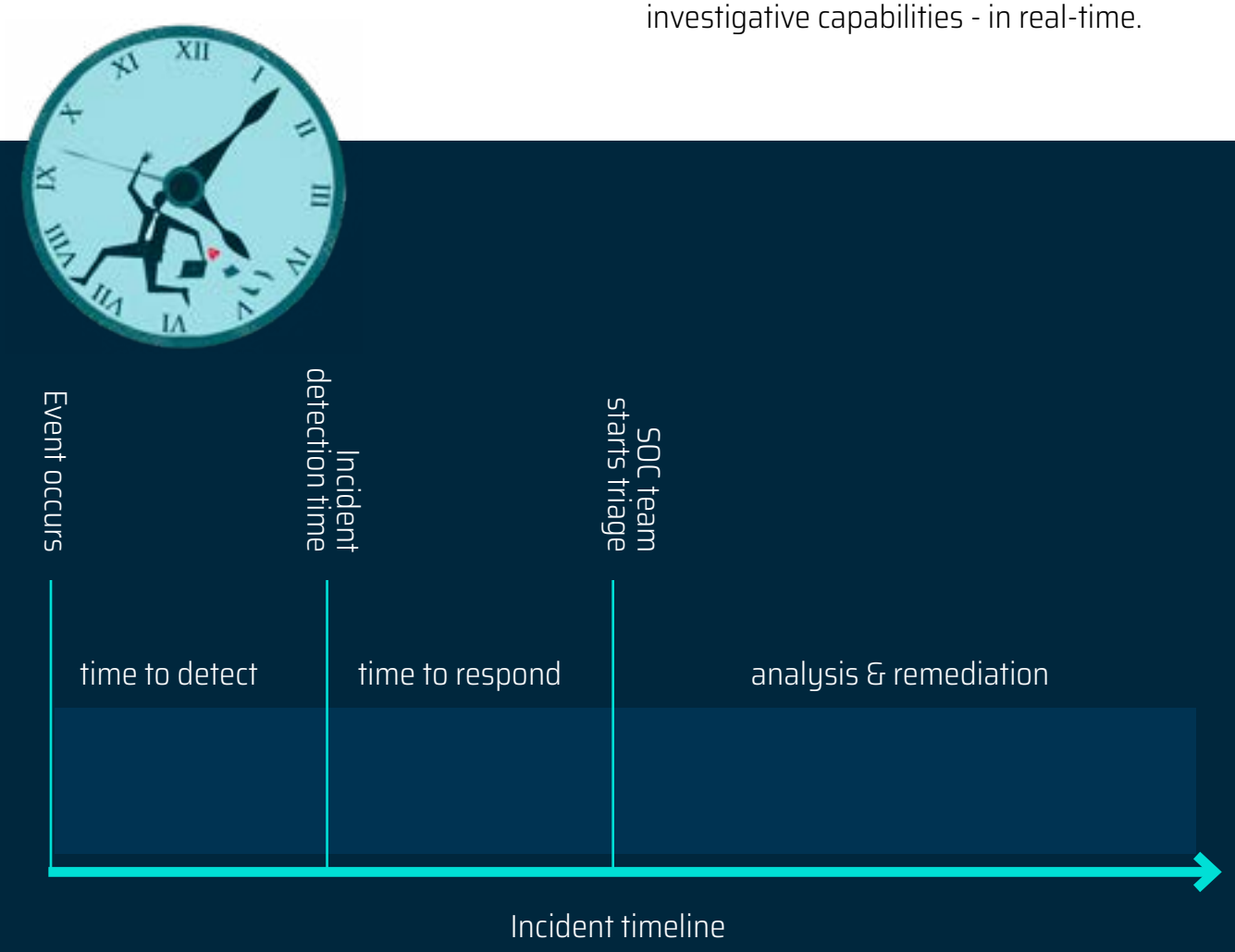
- Blocking attacks before the organization's data or systems are compromised
- Quickly triaging and investigating threat alerts
- Shortening an attack's dwell time

A NEED FOR SPEED

Dwell time represents the length of time a threat actor has free reign in an environment before they are detected, from the moment of initial compromise and until the threat is identified and eradicated.

Dwell time is determined by adding Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR). Lengthy dwell times provide attackers ample opportunity to establish persistence inside your network, giving them free rein to move laterally throughout your infrastructure, perform reconnaissance, and gain access to private client and employee information, funds, and other sensitive data.

Cybersixgill's extensive collection of deep and dark web threat intelligence, when embedded into the SOC's workflow, can act as a force multiplier, maximizing the security team's effectiveness. It is the only offering that provides SOC teams with fully automated threat intelligence and deep dive investigative capabilities - in real-time.



THE CYBERSIXGILL ADVANTAGE

- **Machine Learning Data Enrichment Process:** A sophisticated algorithm that correlates intel items with client assets, compiling patterns and profiles of dark web threat actors and their interactions with peers across platforms, driving proactive and actionable mitigations and improvements based on relevant intel, and ultimately, enhancing resilience to future threats.
- **SaaS Visualized Investigative Portal:** In a centralized, searchable dashboard, analysts gain real-time contextual visibility into the underground threat landscape, with the ability to perform deep-dive investigations across hundreds of millions of intelligence items, including historical data dating back to the 90s, deleted posts, invite-only messaging groups and millions of threat actor profiles.
- **Contextual and Actionable:** With automatic extraction & prioritization as well as alerting and monitoring tailored to each organization's assets and needs, security teams are able to understand the context regarding how each event is related to the tactics, techniques and procedures (TTPs) of specific threat actors, ensuring they take the right action - fast.

CYBERSIXGILL THREAT INTELLIGENCE BENEFITS

- Integrate and customize an automated feed of malicious indicators of compromise (IOCs) that threaten your organizational assets, extracted and delivered in real-time with actionable recommendations for preemptive remediation.
- Receive early warnings of new malware-based threats under development, before they are deployed by threat actors.
- Enrich IOCs with the essential information and context needed to rapidly triage and investigate specific threats or incidents, including dynamic attributes such as where they are trending, POC exploit details, and more.
- Level up your threat hunting for malicious IOCs in corporate networks.
- Get actionable insights to effectively mitigate active threats, earlier on the cyber killchain.
- Harness Cybersixgill's Investigative Portal to probe threat actors and underground chatter to facilitate incident attribution, perform root-cause analysis and understand the trends, targets and motives behind each threat.
- Automatically integrate IOCs into other SOC tools such as TIP, SIEM, XDR, SOAR and VMs.

REMOTE DESKTOP PROTOCOL (RDP)

THE #1 WAY TO GET ATTACKED

What do 1,500 RDP connections have in common? They are all for sale, right now, on the dark web. These compromised RDPs not only pose a threat to the organization to which they belong, but rather, could serve as a springboard to launch attacks against any other target - with attackers exploiting the free resources to host a C2 server, malware, or a proxy to forward an attack. Fortunately, Cybersixgill provides a solution, autonomously monitoring the deep and dark web to identify potentially exposed RDP servers in real-time. By leveraging advanced warnings about emerging threats before they materialize, organizations can take immediate action before it's too late, preventing the cost, damages, and legal repercussions that come with giving in to ransomware extortion.

RDP is a tool developed by Windows, allowing users to remotely connect to and control another Windows PC or server over the internet or on a local network, giving them full access to all tools and software installed on the device. When secured with a strong password and multi-factor authentication, RDP enables employees to securely access corporate resources remotely. However, without proper security measures in place, attackers can compromise these connections and gain access to the exposed server, enabling them to easily deploy ransomware across the network.

THE VAST MAJORITY OF ALL RANSOMWARE ATTACKS GAIN ACCESS TO A VICTIM'S NETWORK THROUGH A "BACKDOOR" APPROACH, EXPLOITING WEAKNESSES IN THE RDP SOFTWARE OR THE WAY IT IS DEPLOYED. [1]

[1] "RDP, the ransomware problem that won't go away,", MalwareBytes (Blog), Feb 16, 2021

REDUCE YOUR RDP ATTACK SURFACE WITH CYBERSIXGILL THREAT INTELLIGENCE

With the sudden transition to remote working practices as a result of the COVID-19 pandemic, a massive proliferation of unsecured RDP connections have flooded the cyber threat landscape. Cybersixgill's Darkfeed empowers organizations to better protect themselves against this mounting threat, including compromised RDP servers with complete IP addresses within its continuous stream of malicious IOCs. This enables you to automatically block these exposed addresses moments after they appear on the dark web, before they are used against your organization.

TIMELY ACTIONABLE INTELLIGENCE. PERIOD.

COMPREHENSIVE
CONTEXTUAL
PREEMPTIVE

So, how worried should you be about compromised RDPs in today's world, and how can you protect your company or organization?

Download Cybersixgill's report, Remote Desktop Pandemic, which provides more insights into the ransomware ecosystem, the danger posed by compromised RDP servers, and practical steps you can take to stay safe.

LEAKED CREDENTIALS

STOP THE LEAK AT THE FIRST DROP

2021 has been the worst year on record for cybersecurity attacks, with account takeover (ATO) attacks - including credential stuffing and phishing attacks - constituting the number one cause of breaches. Once siphoned out of your organization's databases, where do these leaked credentials end up? By now, the answer should be obvious: for sale on the dark web, of course.

AMONG AN ALMOST NEVER-ENDING PRICE LIST, UNDERGROUND MARKETPLACES SHOW BANK LOGIN CREDENTIALS COST AN AVERAGE OF $25 USD; FULL CREDIT CARD DETAILS SELL FOR A PRICE BETWEEN $12-20; AND FOR A MERE $1,275, ONE CAN PURCHASE ENOUGH SENSITIVE INFORMATION TO STEAL AN INDIVIDUAL'S IDENTITY.

INSTANT RESPONSE IS CRITICAL

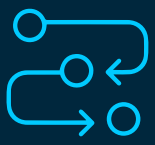
Nothing is faster than real-time. Cybersixgill catches events as they emerge on the underground, before attacks are deployed or leaked credentials are sold. With this unmatched extraction speed, Cybersixgill is truly your best source for fresh intelligence.

Account takeover (ATO) attacks have become a popular weapon of choice for fraudsters, with credentials becoming more easily discoverable and exploitable through the use of bots and malicious automation. In order to overcome this type of attack, one must fight machine with machine. With cybercriminals weaponizing machine learning and artificial intelligence to launch sophisticated cyberattacks, you'd better ensure your cyber defense system is automated as well. This is especially important when protecting cloud assets, which might only be secured with access control security mechanisms.

CYBERSIXGILL ADVANTAGE

GAIN ACCESS

to the largest collection of leaked credentials on the market



RECEIVE CONTEXTUAL AND ACTIONABLE

intel in near-real-time

EASILY SET-UP CUSTOMIZED ALERTS

to be notified when your credentials are leaked

IMPLEMENT AUTOMATED REMEDIATIONARY ACTIONS

to reset exposed credentials as they are detected

SEARCHABLE AND INTUITIVE

Cybersixgill understands how critical each threat or breach can be for your organization, and knows how to prioritize the mitigation process. It provides you with insights about threat status, asset criticality, and actions required for remediation.

TAKE ACTION

Cybersixgill provides real-time, actionable alerts customized to your organization. Deep dive into any escalation in real-time and get a complete picture to fully understand the context. Research threat actor's profiles, MO, and history. Review and analyze across languages, sites, timeframes, types of products, topics, entities, and more.

CONNECT THE DOTS. READ BETWEEN THE LINES. KNOW WHAT'S OUT THERE.

Empower your teams to detect phishing, data leaks and fraud – better. Level-up vulnerability assessment, enhance incident response, and provide stronger brand protection with exclusive access to the most comprehensive, fully automated collection available from the deep and dark web that includes closed access forums, instant messaging apps, paste sites, and more.

7X
DETECTION
of leaked Credentials

10X
COLLECTION
from dark web sources

13X
COLLECTION
from instant messaging apps

24X
FASTER
extraction

POWER BEYOND COMPARE

	CYBERSIXGILL 100% AUTOMATED	OTHER SOLUTIONS Manual, back-office "detection"
Avg. detection time	Seconds	Days/Weeks
Time from setup to relevant data	Minutes	Days
Collection from dark web sources (forums, markets)	Hundreds of sources	Dozens of sources
Speed of data extraction & enrichment	Quick. Automatic.	Slow. Manual.
Collection from instant messaging apps	10s of millions. Automated, in real-time.	A million at best. Manual.
Image/ OCR extraction	Yes	No
Multi language support	Any language	Depends on analyst
Data-driven insights	Yes	Yes
Global reach	Yes	No
Scalability	Instant	Weeks - Months

VULNERABILITY PRIORITIZATION

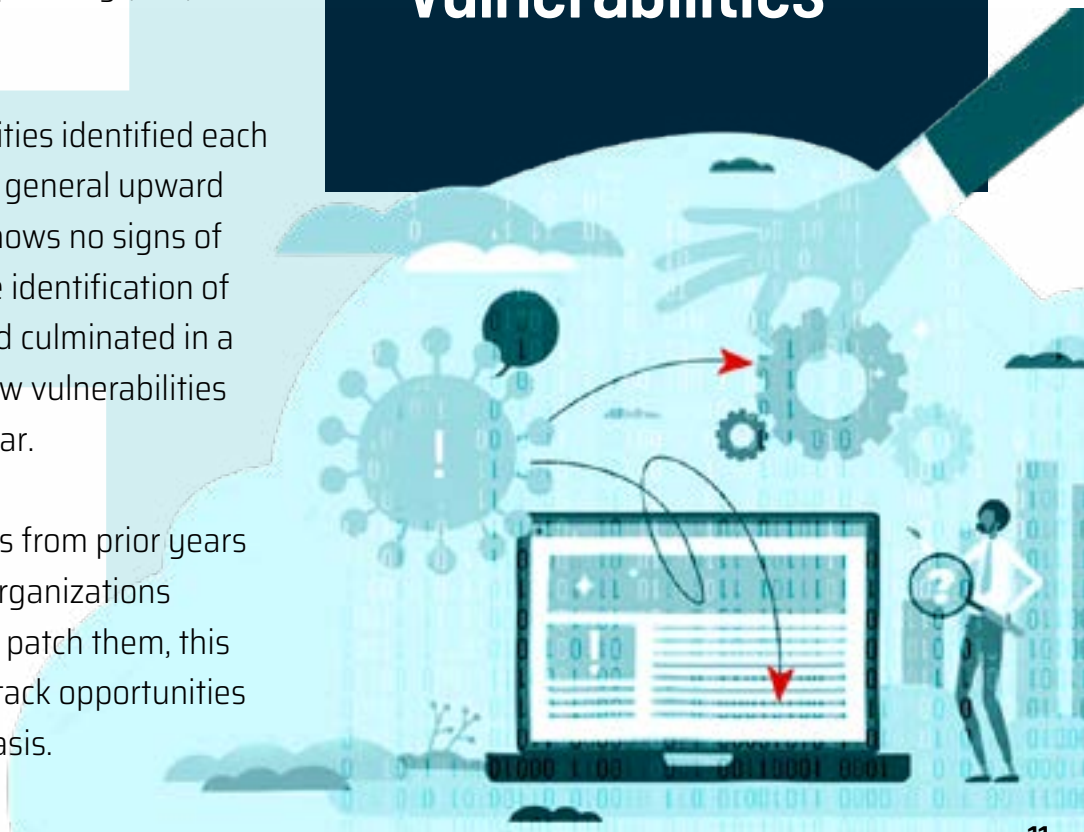
AGILE VULNERABILITY MANAGEMENT

When browsing the available stock on the cybercriminal underground, threat actors enjoy an endless supply of vulnerabilities to choose from, while their counterparts on security teams face more potential security holes than they can patch. In IBM's 2021 X-Force Threat Intelligence Index, vulnerabilities surpassed phishing as the most common attack vector, whereby vulnerability exploitation (35%), surpassed phishing (31%) for the first time in years.

#1 attack vector is now the exploitation of vulnerabilities

The number of new vulnerabilities identified each year has continued to rise in a general upward trend since 1988. This trend shows no signs of abating - 2020 began with the identification of 18,000 new vulnerabilities, and culminated in a grand total of over 159,000 new vulnerabilities identified by the end of the year.

As cybersecurity vulnerabilities from prior years continue to pose a threat for organizations that have not yet caught up to patch them, this cumulative effect increases attack opportunities for threat actors on a yearly basis.



GAIN THE ADVANTAGE BY BECOMING AGILE

Accelerate prioritization and remediation with the most comprehensive collection of vulnerability-related threat intelligence from the deep and dark web, and the only solution that predicts the likelihood of vulnerability exploitation over the next 90 days.

Derived from automated AI analysis of underground discourse, the Cybersixgill Dynamic Vulnerability Exploit (DVE) Score provides an accurate and real-time assessment of the immediate risks of each vulnerability based on threat actors' intent. It also contains actionable information and context for clear visibility into the score, empowering customers to confidently rank vulnerabilities and prioritize patching decisions in order of urgency and in light of real-time threat intelligence. Cybersixgill Investigative Portal users can further investigate to learn more about CVE popularity, potential exploit codes, attributes, score history, relevant actors, and more.

VULNERABILITY INSIGHTS

REAL-TIME PERFORMANCE

Know an exploit is published or a vulnerability is discussed before threat actors even think of using it

COMPREHENSIVE QUALITY COLLECTION

Omni-channel collection sourced from the largest collection of vulnerability-related threat intelligence

PREDICT EXPLOIT PROBABILITY

Track threats from CVEs that have a higher probability of being exploited by active threat actors in the cyber underground

TAKE THE RIGHT ACTION

Leverage insights that allow proactive remediation and prevention

THE SCORE THAT TELLS YOU MORE

The vast majority of exploitation happens on the first day of a vulnerability's public release. It is therefore crucial for security teams to understand on a real-time basis the urgency and severity of each threat.

The DVE Score allows security teams to see true threats as they emerge, saving crucial time as potential threats materialize into active ones. It provides an extra-layer of real-time context that empowers security teams to better prioritize their workload and manage their patching cadence.

BRAND PROTECTION

HOW DO YOU PUT A PRICE ON YOUR REPUTATION?

Cybersixgill is the only solution that is comprehensive, covert and fully automated. It empowers security teams with the insights they need to proactively protect their critical assets, prevent fraud and data breaches, protect their brand, conduct investigations in real-time and minimize attack surface. Seamlessly integrated into existing security stacka, Cybersixgill delivers clear visibility into the organizational threat landscape coupled with contextual and actionable recommendations for remediation.

It is important to understand the common threats in order to defend against them.

BRAND IMPERSONATION

- **Email -** Impersonation of a company's email accounts (through spoofing or compromised email credentials) in order to steal credentials or other sensitive data. By posing as the brand through email, attackers can trick the recipients into clicking on a malicious link or attachment in the email, which in turn can lead to data theft, credential theft, financial theft or malware/ ransomware infection.
- **Phishing Websites** - Phishing websites imitate the brand's look and feel in order to trick users into submitting their login information that later can be leveraged for malicious purposes.
- **Social Media** - Creating fake or compromised employee accounts, often targeting the executive management team and VIPs, in addition to impersonating or compromising corporate social media accounts.
- **Website Defacement** - Breaching the company website with their own content or messages.

DATA LEAKAGE

- Exfiltrating or exposing personally identifiable information (PII) and corporate intellectual data that can cause significant damage to the brand's reputation.

RANSOMWARE

- Reputational damage
- Negative impact to customer loyalty & trust
- Disruption of business operations and denial of products and services
- Immediate and long term financial impact

HOW DOES CYBERSIXGILL THREAT INTELLIGENCE KEEP YOUR BRAND SAFE?

Cybersixgill enables organizations to build an effective cyber-defense against attackers, providing proactive solutions that help to mitigate damage to brand, reputation and their bottom line.

By receiving insights ahead of time, SOC teams are able to plan ahead, predicting emerging threats and acting preemptively, rather than reactively, to block attacks that threaten their organization. This empowers teams to maximize their efficiency and efficacy, greatly reducing detection and response time.

CYBERSIXGILL ADVANTAGE

- **Continuous monitoring** of surface, deep and dark web sources in real-time to act as an early warning system. This includes but is not limited to: onion sites; forums; invite-only messaging groups; social media; and various underground marketplaces.
- **Enhanced detection** by keeping SOC teams up to date with the latest risks and attack methods, as well as actionable reccomendations to protect against them.
- **Rapid response** by having actionable insights and contextual data to make security investigations as efficient and effective as possible.

Today's SOCs face an uphill battle in changing the cyber threat equation in their favor.

To gain the upper hand in the cybersecurity arms race, cyber threat intelligence is not a luxury, but a necessity. It's time to include actionable intelligence from underground sources to improve your SOC's performance.

ABOUT CYBERSIXGILL

Cybersixgill brings agility to cyber defense, with fully autonomous threat intelligence solutions to help organizations proactively detect and protect against phishing, data leaks, fraud, malware and vulnerability exploitation - enhancing cyber resilience and minimizing risk exposure in real-time. The Investigative Portal provides covert access to threat intel from the deep and dark web, complete with context and actionable insights for remediation. Seamlessly integrated into existing security systems, Darkfeed™ enriches endpoint protection by preemptively blocking malicious IOCs, while CVE insights from the DVE Score™ transform vulnerability management, predicting the immediate risk of vulnerability exploitation based on threat actor intent. Current customers include global enterprises, financial services, MSSPs, government & law enforcement entities.