cybersixgill

FIXING THE BROKEN MIDDLE

How the Cybersixgill DVE Score Helps Prioritize Vulnerabilities

Introduction

When it comes to cybersecurity, the trends affecting today's businesses and organizations are both frightening and encouraging. In many cases, however, they are simply overwhelming.

Cyberthreats are constantly advancing, and the rate at which the public learns about newly discovered vulnerabilities is increasing. The problem is that installing patches tends to be a costly and time-consuming process, and many organizations are unable to keep up with all of the relevant patches.

It is critical for cybersecurity professionals to prioritize the vulnerabilities that pose the greatest risk in the short term. However, organizations typically struggle to effectively determine which vulnerabilities are the most urgent—preventing them from prioritizing the most important patches.

In response to this challenge, the Cybersixgill Dynamic Vulnerability Exploit (DVE) Score makes it easy for businesses and organizations to identify the vulnerabilities presenting the greatest risk over the next 90 days. By evaluating chatter on underground forums and intelligence from various other sources in real-time, Cybersixgill's AI-powered scoring engine estimates the likelihood of a given vulnerability being exploited in the near future. Then, it considers this probability when assigning a score to that vulnerability. This approach empowers organizations to confidently rank their vulnerabilities in order of their urgency in light of real-time threat intel, so that they can make sure to install the most pressing patches first.

How troublesome is the challenge of identifying urgent vulnerabilities? How does Cybersixgill gather data, analyze it, and evaluate any given vulnerability? And how effectively does this technology address key cybersecurity issues facing today's businesses and organizations? This paper will answer these and other essential questions about the Cybersixgill DVE Score, shedding light both on this innovative solution and on the pressing problems it is designed to solve.

Why prioritizing vulnerabilities is essential for cybersecurity

The numbers show that the pace at which cybersecurity vulnerabilities are discovered is increasing over time. The good news is that patches are typically announced at the same time as the vulnerabilities they address. The problem is that organizations simply do not have the time or resources to install every patch.

How widespread and alarming is this problem? In 2020, yet again, more cybersecurity vulnerabilities were discovered than the year before. Specifically, 18,353 new vulnerabilities were added to the National Vulnerability Database (NVD), including a record number of 4,381 high-severity vulnerabilities over the course of the year—an average of 12 every single day.

These unpatched vulnerabilities are one of the biggest sources of data breaches and other risks for companies and organizations. As of 2018, according to Ponemon, 60% of organizations that had suffered

a data breach in the previous two years cited as the culprit a known vulnerability for which they had not yet patched.

The life cycle for typical vulnerability management, pictured below, represents a process framework for monitoring, planning, and maintaining security programs that address these risks. The three-part paradigm that underlies the cycle—SEE, PRIORITIZE, and ACT to address risk—provides the basis for business-aligned security operations.

The time-consuming burden of patching

The real challenge here is the necessary patching. If this process were easier, by now vulnerabilities would have been relegated to a lower gear of security control, just like antivirus and other such measures. However, vulnerability patching is a complex process that is usually managed by teams outside of security organizations, and it is time-consuming. In fact, Ponemon has found that it takes **an average of 12 days** for teams to coordinate and apply a patch across all devices.

Beyond the time and resources involved in applying patches, some managers are reluctant to apply them for other reasons. A whopping **72% of managers are afraid** to apply security patches right away because they could “break stuff.”

Simply put, vulnerabilities are being created and discovered at a record pace, creating unprecedented risk—while the mechanism to mitigate that risk (patching) is severely constrained.

This problem is exacerbated by improper prioritization of vulnerabilities. Nearly two thirds of all companies **(65%) say that it is currently too difficult** for them to decide correctly on the priority level of each software patch (in other words, to determine which update is of critical importance and should therefore be applied first).

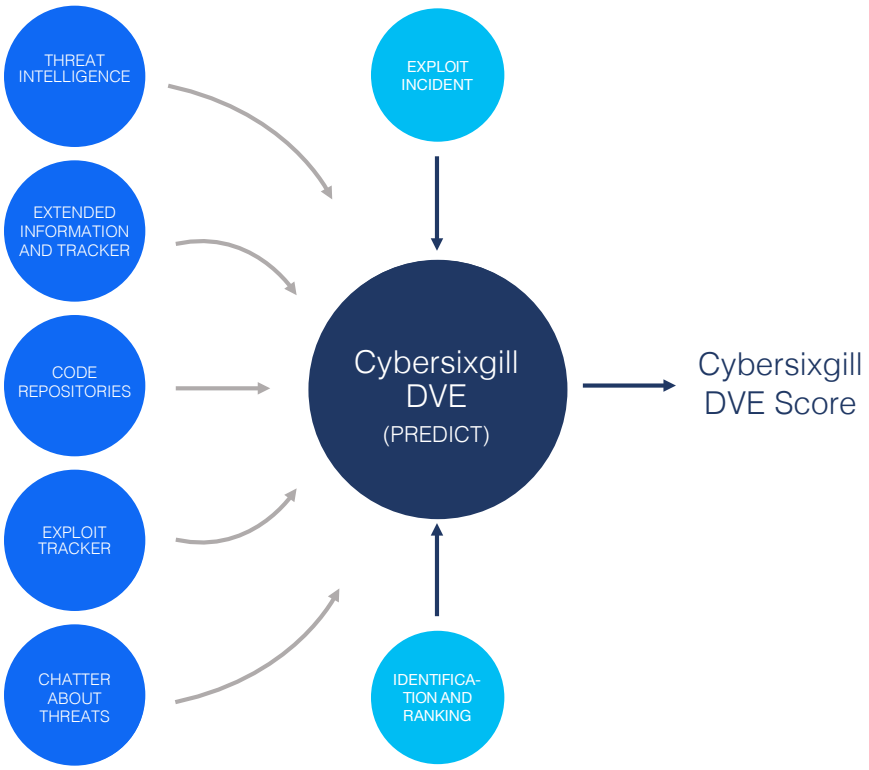
How the Cybersixgill DVE Score helps

To meet this need, the Cybersixgill DVE Score predicts the probability of a CVE being exploited in the near future. The scoring system is dynamic, reflecting the likelihood that threat actors will take advantage of a given vulnerability in the next 90 days. This information then enables cybersecurity, VM, and IT teams—as well as CISOs—to focus on their most pressing vulnerabilities.

Because the DVE Score takes a comprehensive and dynamic approach to evaluating vulnerabilities, companies and organizations can confidently make it a major factor they use when deciding which patches to apply and in what order.

How the scoring engine works

Cybersixgill's AI-powered engine automatically calculates scores for specific vulnerabilities by analyzing a rich variety of intelligence sources. This approach enables the DVE Score to reflect the most current intent of potential attackers. It also allows for the identification of CVEs that others define as irrelevant or obsolete, but have a high probability of being exploited in the short term by active threat actors in the cyber underground.



Why it's so difficult to prioritize vulnerabilities effectively

There's an open secret in the world of cybersecurity: most of the prioritization of vulnerabilities is driven by CVSS scores. While these scores can evaluate the severity of a given vulnerability, they do not adequately factor in the question of how likely that vulnerability is to be exploited in the first place. Moreover, CVSS scores rarely change and do not reflect the state of threat actor's intent.

Not only does this system often result in outdated CVSS scores, but it can delay an organization's response to a discovered vulnerability—even as attackers can get to work trying to exploit that vulnerability.

The combination of stale CVSS scores and the wait for a score to be assigned leaves too many security teams with a limited understanding of their risk environment. Meanwhile, vulnerability overload makes it even more difficult for security teams to prioritize their remediation efforts. Consequently, approaches to security tend to be more reactive than proactive and more tactical than strategic. In particular, it can be difficult to align organizational priorities with the threats posed by potential attackers.

To enable cybersecurity teams to prioritize patches as quickly and effectively as necessary, they need a different way to evaluate specific vulnerabilities. They need a solution that actively incorporates attacker capability, intent, and interest—and that does it all in real-time.

The Cybersixgill DVE Score is calculated based on several parameters:

- **When was the CVE published?**
  CVEs which were published more recently will have a higher probability of being exploited by threat actors.

- **Does the CVE have a proof-of-concept exploit code on GitHub?**
  Threat actors are lurking for POC exploit codes in code repositories such as GitHub, waiting for an opportunity to use them as part of their malicious campaigns.

- **Does the CVE have a proof-of-concept exploit code offered on underground forums?**
  Exploit codes are also bought and sold on dedicated markets on the dark web, allowing less sophisticated actors to execute advanced attacks.

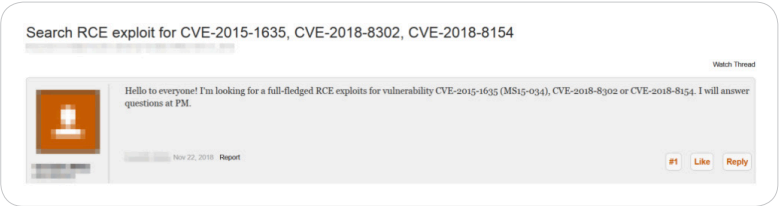
- **Was the CVE discussed on the dark web or the clear web?**
  CVEs that are the subject of discussions on the deep and dark web are more likely to be exploited by threat actors. The volume of discussion about the CVE and how recently these discussions took place are key factors in determining the exploit probability of the CVE.

- **How strong is the reputation of the forum where the POC code was shared?**
  Different actors congregate in different forums. Some forums attract more reputed actors and consequently, any information from these forums would carry more weight.

- **How reputable is the threat actor? How long have they been active? Who is in their social network?**
  Cybersixgill applies machine-learning algorithms to calculate reputation score for each threat actor. Cybersixgill incorporates multiple elements such as actor's tenure, their social network, the strength of their social network etc..

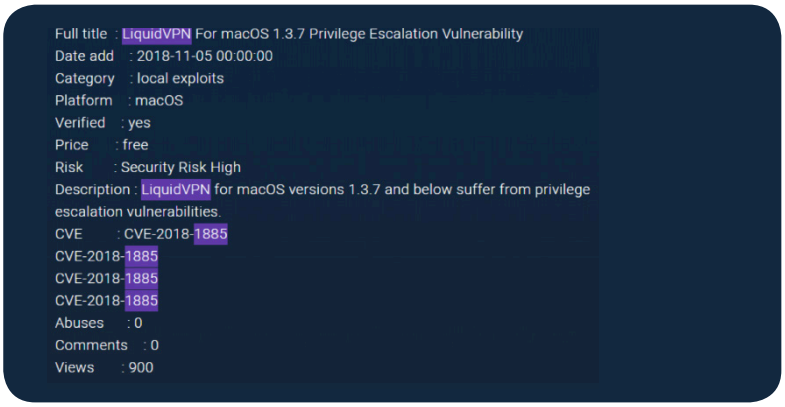
This intelligence is sourced from multiple places, including:

- **Underground forums**
  Forums on the deep and dark web are key places where threat actors discuss recently revealed vulnerabilities, share exploit codes, and even plan joint attack campaigns designed to take advantage of these vulnerabilities. To effectively utilize intelligence from these sources, organizations need a solution that automatically extracts large amounts of information and analyzes them rapidly.



- **Underground markets**

  Marketplaces on the dark web are used as meeting places for buyers and sellers of exploit code kits, the Metasploit framework, and other malicious tools. Therefore, extracting information from an illicit trading platform and converting it into structured data should play a prominent role in any cyberthreat intelligence (CTI) solution intended to solve the CVE prioritization challenge.



- **Code repositories**

  Proof-of-concept (POC) exploit codes are published daily on GitHub "for educational purposes only." Threat actors lie in wait for such golden opportunities, and such POC codes attract significant interest from the malicious actors who look to exploit them.

- **Social media**

  Many users on Twitter, Telegram, and other social media platforms share links to POC exploit codes and updates regarding CVE exploitability trends. Tracking the discourse on these platforms provides early warning regarding new exploits and vulnerabilities.

- **Paste sites**

  Threat actors share large chunks of text on these sites, sometimes including golden nuggets such as Metasploit tools, exploit codes, and references to various CVEs.

- **Blogs, cybersecurity websites, and technical feeds**

  These sources can provide indications that a given CVE has already been used as part of an attack ("a weaponized CVE"), an indication that it is likely to be exploited again.

How this approach helps prioritize vulnerabilities

By offering a system of evaluating vulnerabilities that goes beyond that of CVSS and other solutions, the Cybersixgill DVE Score offers companies and organizations a more effective way to identify the most urgent patches to implement. Ultimately, the key benefit of this scoring system boils down to the accuracy of its predictions.

At the heart of Cybersixgill's accuracy is a predictive model based on proven data science techniques that have been tested and validated in many security and non-security use cases. This model automatically evaluates the chronology of the evolving life story of each CVE, with scores computed in near real-time.

Conclusion

Given the cyberthreat landscape facing today's businesses and organizations, they are well served by the frequency with which patches are released to address their cybersecurity vulnerabilities. Especially in light of the high-profile and costly cyberattacks that have grabbed headlines in recent years, the availability of patches should enable cybersecurity professionals to improve their level of defense.

The problem is that implementing these patches requires significant time and resources, and their sheer volume makes it virtually impossible for typical organizations to keep up with all of them. For these organizations, the best viable option is to patch the most urgent vulnerabilities—if they can identify them. But even evaluating the urgency of a given vulnerability is in itself a major challenge, and in the fast-moving world of cybercrime and cybersecurity, a vulnerability's level of urgency can change suddenly and rapidly.

Cybersixgill addresses this hurdle by automatically evaluating the urgency level of specific vulnerabilities. Cybersixgill's AI-powered scoring engine analyzes various threat intelligence sources including the underground forums of the deep and dark web, using this information to evaluate the likelihood of a given vulnerability being exploited in the next 90 days. And because scores are updated frequently, they enable organizations to keep up with the latest threat intelligence.

Moreover, by tapping into the dark web's value as a source of cyberthreat intel, the Cybersixgill DVE Score takes into account footprints that bad actors often leave behind as they communicate about their plans in underground forums. Because the dark web is where threat actors go to communicate online when they want to stay anonymous, it is often the first place where evidence of a future cyberattack appears. And, with the world's largest data lake of information from the cyber underground, Cybersixgill is uniquely capable of finding and utilizing this type of intelligence.

How does all of this help companies and organizations stay safe? It empowers them with the information they need to make well-informed decisions about which patches to implement first. Although the Cybersixgill DVE Score does not in itself remove the vulnerabilities these organizations face, it gives them the insights they need to set their priorities effectively based on the latest online discourse—so that they can install the right patches at the right times to protect themselves. In short, the DVE Score offers them a reliable way to keep up with the most urgent patches.