BITSIGHT

REPORT

A Global View of the CISA KEV Catalog: Prevalence and Remediation

Author: Ben Edwards

Date: May 2024

Table of Contents

Key Points

- **The KEV catalog is growing.** The KEV catalog is an indispensable source of information, and one that is growing at a rate of 17 new vulnerabilities per month in 2023.
- **KEVs are common and more prevalent compared to other vulnerabilities.** 35% of organizations observed by Bitsight had a KEV in 2023. The median KEV is 2.7 times more prevalent in internet facing systems than other vulnerabilities.
- **KEV rates vary by industry and geography.** Some KEV vulnerabilities are 10x more likely to appear in certain industries or locations.
- **KEVs get fixed faster than other vulnerabilities.** Half of all KEV detections are resolved in just under 6 months (175 days), compared to well over two years (621 days) for non KEVs, but this is highly dependent on the severity of the vulnerability.
- **Meeting KEV deadlines can be difficult.** The ability for organizations to meet CISA deadlines varies substantially, with some never meeting it and some always meeting it. On average, only 40% of KEVs are remediated by the deadline set by CISA.
- **Binding directives are improving U.S. federal agency remediation rates.** Agencies subject to CISA's binding directives on KEV are 63% more likely to remediate KEVs by their deadlines than other organizations.

Introduction

If you're an information security professional and have been browsing LinkedIn, you have likely seen quite a lot of posts extolling the virtues of the Cybersecurity and Infrastructure Security Agency's Known Exploited Vulnerabilities (KEV) Catalog.[1] Since the KEV catalog's inception at the start of November of 2021, it's been of intense interest to large swaths of the cybersecurity community, particularly those involved in vulnerability management and risk assessment.

So what is this catalog and why are so many people interested in it? The catalog itself was created as part of CISA's Binding Operational Directive (BOD) 22-01, which sought to identify and mandate remediation of vulnerabilities known to CISA to be exploited in the wild and were likely to affect U.S. federal agencies. In fact, U.S. federal agencies are required to remediate the vulnerabilities in the KEV catalog within a given deadline published with the vulnerability.

CISA created the KEV catalog in part because of challenges that organizations have historically faced in prioritizing vulnerabilities. In any given year, there are tens of thousands of new vulnerabilities. But according to CISA, a study of historical vulnerability data dating back to 2019 shows that less than 4% of all known vulnerabilities were being used by attackers in the wild. Given the risk that these particular vulnerabilities present, CISA states that "known exploited vulnerabilities should be the top priority for remediation."

This means the KEV catalog provides a clear risk signal to not just federal agencies but the public at large. After all, vulnerabilities that attackers are actively probing are of primary concern to anyone trying to reduce their organizational risk. Because of its use to organizations and its open nature (the KEV catalog is openly published and regularly updated), it has been the subject of a number of studies, in particular by vulnerability management companies. Bitsight is intensely interested in understanding an organization's capacity to fix vulnerabilities and critical drivers of organizational behavior. In the past, our researchers have published research showing the impact that CISA alerts have on remediation rates. We've even identified new vulnerabilities that have been added to the KEV catalog itself. This study highlights Bitsight's unique perspectives on the KEV Catalog and CISA alert.

[1] Terminology note: We'll refer to the entire Known Exploited Vulnerability Catalog as the "KEV Catalog" and individual entries as "KEV" or "KEVs."

[2] CISA Binding Operational Directive 22-01, Nov. 3, 2021, available at https://www.cisa.gov/news-events/directives/bod-22-01-reducing-significant-risk-known-exploited-vulnerabilities

What Goes in the KEV Catalog

There are three criteria for a vulnerability to make it into the KEV catalog:

Assigned a CVE. The vulnerability must have been assigned a CVE ID from one of the approved CVE Certified Numbering Authorities (CNAs).

Evidence of Exploitation. CISA must have evidence that attackers are actively attempting (successful or not) to exploit the vulnerability. Note that this excludes any simple Proof of Concepts or scanning activity, and is strictly verified evidence of exploitation.

Remediation Available. Remediation must be available to organizations who detect the vulnerability on their system. After all, it wouldn't be much use to warn organizations of danger and give them a deadline if nothing could be done about it.

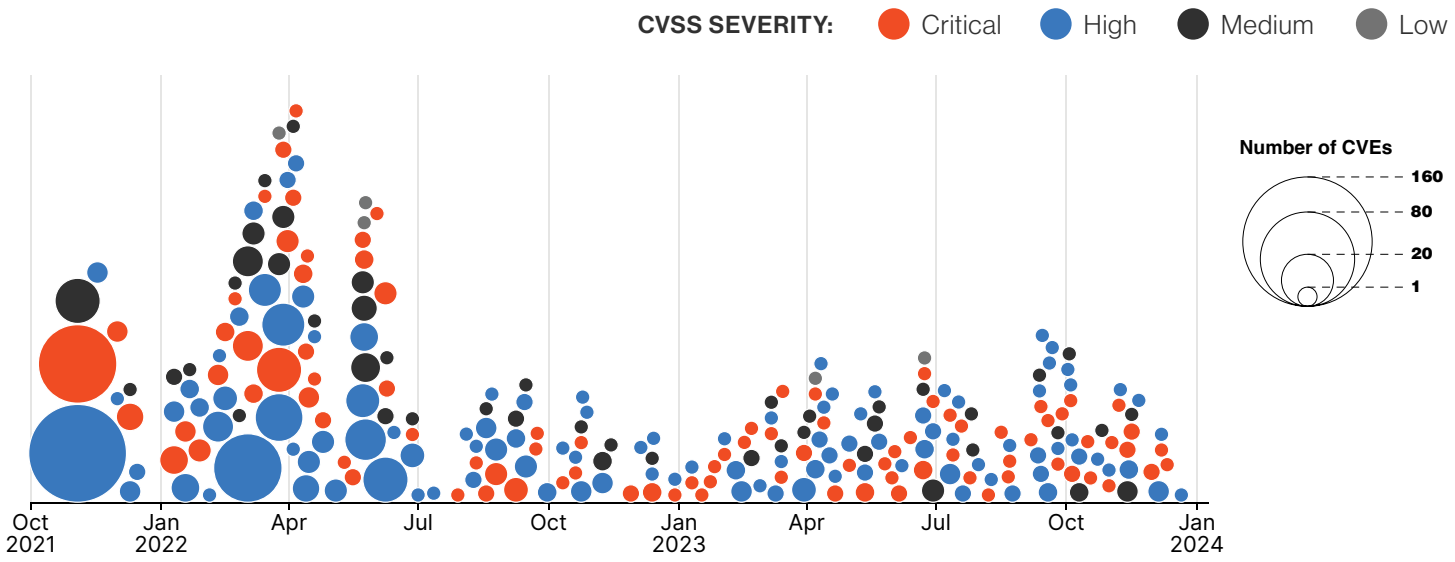
The above are the criteria that CISA states, but there are likely vulnerabilities that fit that criteria but don't make it onto the list. We won't take up time speculating here on why that might be the case, but it's likely that CISA avoids vulnerabilities that are unlikely to affect federal agencies (Minecraft CVE anyone?), or that are not all that widespread.

In addition to the vulnerability, the deadline[3] for federal agencies to remediate, and the required action to be taken for those agencies,[4] the KEV catalog also includes whether the vulnerability has been known to be used in ransomware campaigns. In ***Figure 1***, we show how the KEV catalog has evolved in the last approximately two years.

Initially, there were large additions to the KEV catalog, but we've seen a steady stream since then. In fact, the growth rate is around 17 each month averaging a little more than one every other day. A not insignificant fraction of those (20%) are used in ransomware.

FIGURE 1: Date CVEs were added to KEV Catalog

Each circle here is a day where CVEs were added to the KEV catalog. The color indicates the qualitative CVSS Severity for the CVE and the size is the number of CVEs with that severity added that day.

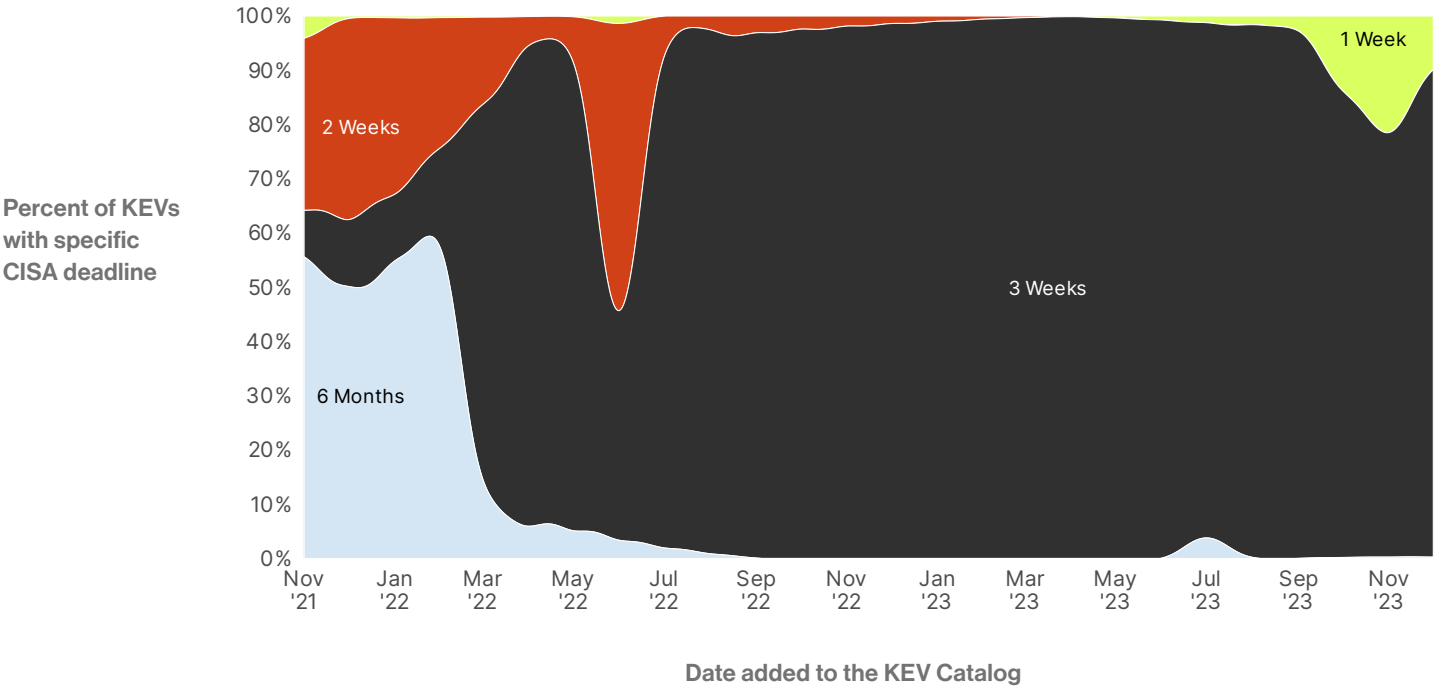


[3] *These deadlines are a specific date since the vulnerability was added to the catalog that agencies must address them. We find that these fall into the 4 categories: 6 months, 3 weeks, 2 weeks, and 1 week. It is unclear why these specific deadlines are chosen by CISA.*

[4] *These deadlines and required actions are only for U.S. federal agencies, but probably are good advice for everyone.*

FIGURE 2: KEVs with specific CISA deadline

Proportion of of vulnerabilities with a specific deadline over time. Data is aggregated monthly. The width of each color indicates the total percentage of vulns with that deadline during the month.

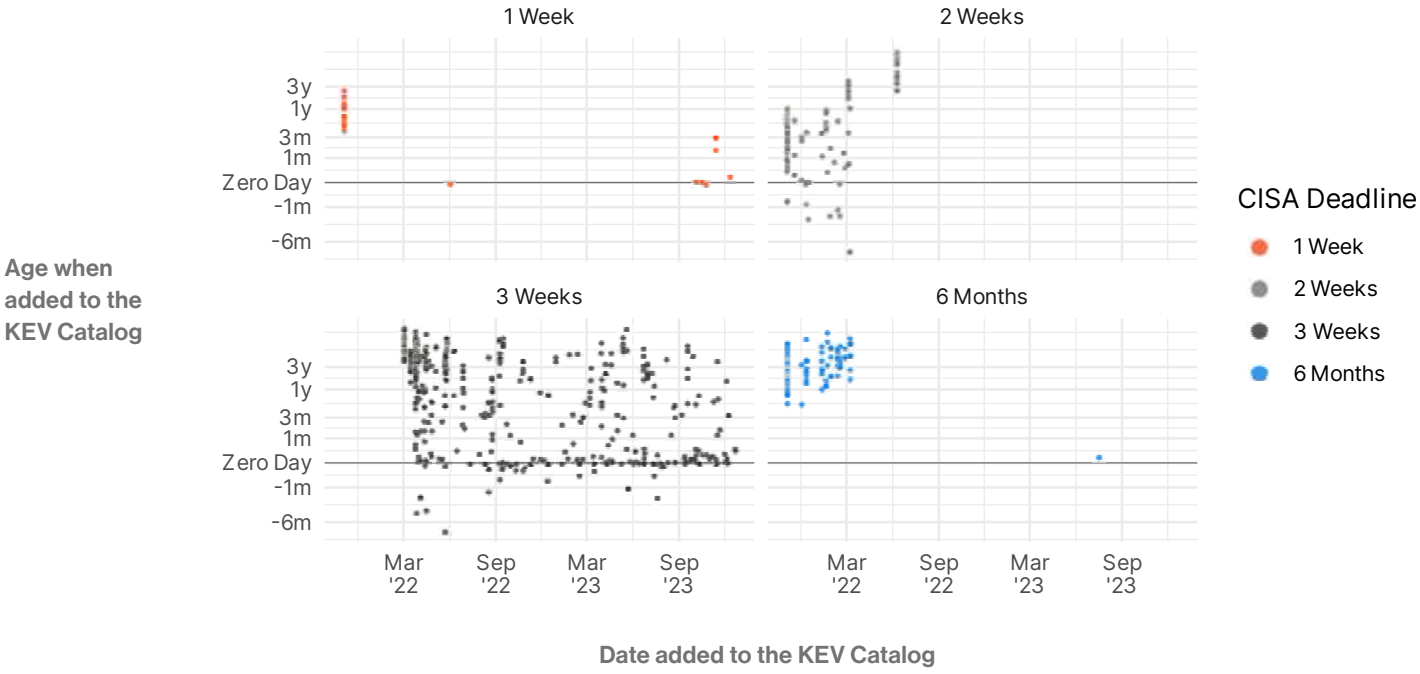


We'd also note a shift in the use of various deadlines in ***Figure 2***. Initially 2 week and 6 month deadlines were common with a handful of 1 week deadlines. But in the late winter and early spring of 2022, a shift to 3 week deadlines was made and since then the catalog has focused primarily on those, with occasional 1 week or 6 month deadlines.[5] Why the shift? Those early vulnerabilities *tended* to be older when they were added to the KEV catalog (***Figure 3***). Given that they may have been around for a while, it seems logical to give organizations time to address issues.

[5] *As is often the case with cybersecurity data, these deadlines are not completely clear cut. There were a number of Emergency Directives published by CISA before the existence of the KEV catalog, and many of the KEV CVEs got attached to those emergency directives, which creates situations where the due date is before it was added to the KEV catalog (sometimes by as much as a year and a half). For those instances, we reviewed the actual emergency directives to see exactly when things were due, and for the most part they were due inside of a week. There are others that are due a little longer than 6 months or 3 weeks as well, but we are going to drop them in the nearest bucket rather than confuse our results with a bunch of 24 or 183 day deadlines.*

FIGURE 3: Age and Date at Addition to KEV Catalog

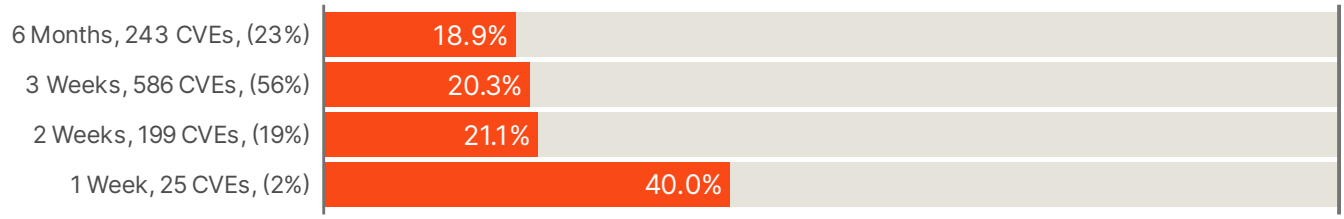
Age of vulnerabilities when it was added to the KEV catalog, broken up by deadline, note the scaling here is a bit odd, we use a log transformed scaled for the positive values, but linear for values < 10.



What's a little strange in the figure above is there are a number of KEVs that were added to the catalog *before* they were published, sometimes by as much as 6 months. Doing some investigation, we found a number of cases in which a vendor will release an advisory and patch on reserved CVE numbers, but the formal publication process is not complete until much later, as was the case with CVE-2021-38000, a Chrome vulnerability that was first disclosed on October 28, 2021, but officially published until November 23.

Deadlines seem to be influenced by whether a vulnerability is used in ransomware: 1 week deadline vulnerabilities are nearly twice as likely to have been used in ransomware[6] (***Figure 4***). This likely is because these vulnerabilities are particularly urgent and likely to cause significant damage if exploited on an agency system.

FIGURE 4: Percent KEVs known to be used in ransomware by deadline



[6] *The criteria by which CISA determines whether a CVE is being used in ransomware campaigns is a bit vague. The data itself grew out of their voluntary Ransomware Vulnerability Warning Pilot, started in March 2023, and made "public" in October of 2023. Similar to how CISA determines "active exploitation", whether an CVE is used in ransomware is determined as "whether CISA is aware that a vulnerability has been associated with ransomware".*

What Bitsight Sees

As we mentioned in the introduction, there has been a lot of analysis of the KEV catalog and what security technology vendors' particular data can tell us about the state of risk. Other vendors have focused strictly on the data in the KEV catalog itself or when they were discovered by endpoint vulnerability management technology. These contributions have been positive but they are limited to observations made on customers who happen to have installed a particular scanning service.

Bitsight has unique perspectives on these vulnerabilities. Bitsight's technology scans the entire Internet, allowing us to assess a broader community of organizations and sectors and more accurately reflect KEV prevalence across the globe. Our view isn't completely omniscient; we are generally restricted to devices that are Internet facing, and to those vulnerabilities that can be exploited over the Internet.[7] This means that we'll almost never be able to see client side software, but on the other hand it's also the view of organizations most attackers will be starting from.

35% of organizations had 1 KEV in 2023

66% of organizations that had a KEV had more than 1

10% of organizations that had a KEV had more than 10

For purposes of this study, we are going to focus on a sample of ~20% of the current KEV catalog, which is a subset of vulnerabilities that Bitsight can and currently detects.

KEV Prevalance

In reviewing the security posture of more than 1 million global organizations, **35.3% had a KEV in 2023**. That means at one time or another more than a third of organizations had an externally facing CVE that was known to be exploited in the wild.[8]

Obviously, just asking whether an organization has *any* KEV is a pretty blunt question. After all, some organizations likely experience dozens at one time or another and some might only have one. Let's see if we can sharpen our analytic tools a bit to see if we can better understand what it actually means. For example, the next question is exactly how many unique KEVs Bitsight detected on organizations' assets over the course of 2023? Among the 35.3% that had any, most (about 2/3rds) experienced more than one, and a quarter experienced more than 5 (***Figure 5***). One thing to note though is that the counts below are "heavy tailed"— meaning that many organizations experience a few, while a small, but not insignificant minority experience a lot. In this case that means about 10% of organizations had 10 or more unique, internet facing, detectable known exploited vulnerabilities over the course of 2023.

But again, we are being a little blunt and maybe we can use one more pass of the whetstone on our measure to see if we can refine things based on time. That is, it's possible that an organization could have one KEV on one day or one KEV every day, certainly the latter would be worse. In ***Figure 6***, we examine the weekly average over the course of 2023.

[7] *Bitsight also only scans for vulnerabilities using non-intrusive techniques. This an ethical decision made as a company a long time ago.*

[8] *This isn't a totally straightforward calculation as it might seem. The KEV catalog grew over the course of 2023 as did Bitsights capabilities. Check out appendix Figure A1 for some details.*

FIGURE 5: Distribution of number of unique KEVs detected in organizations in 2023

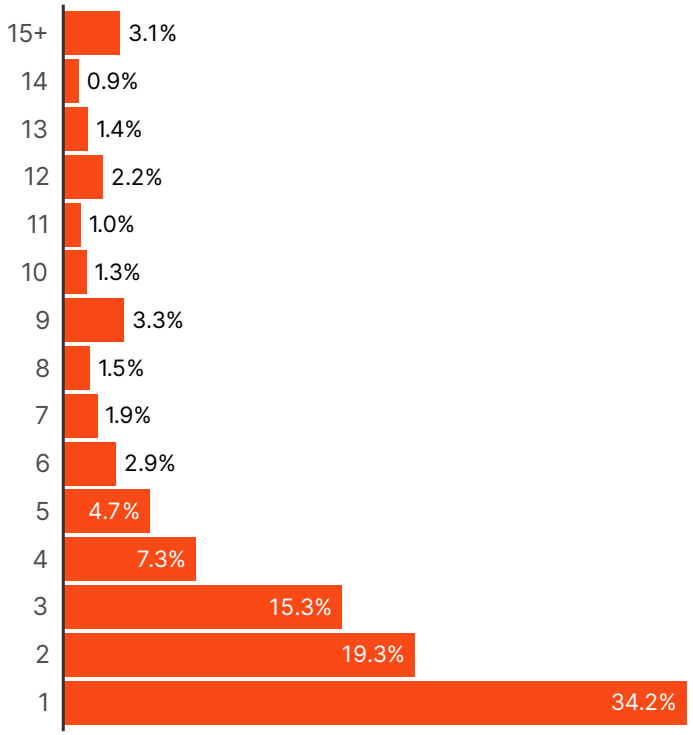
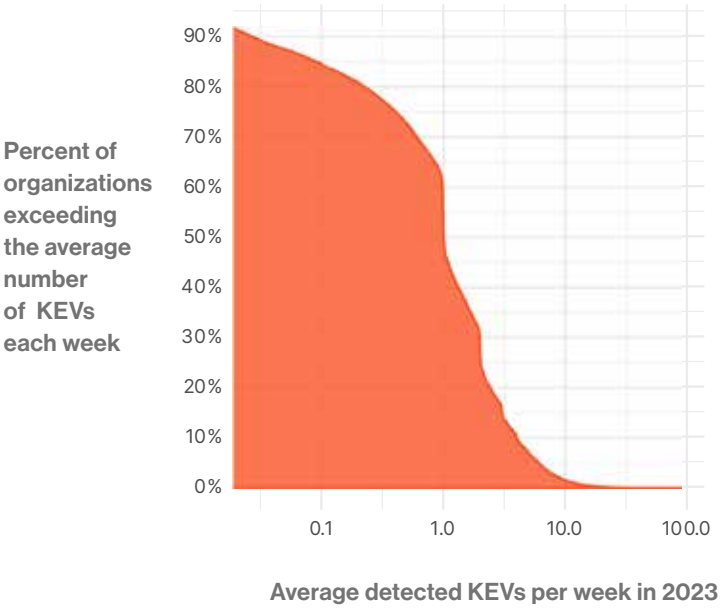


FIGURE 6: Percent of organizations exceeding the average number of KEVs each week

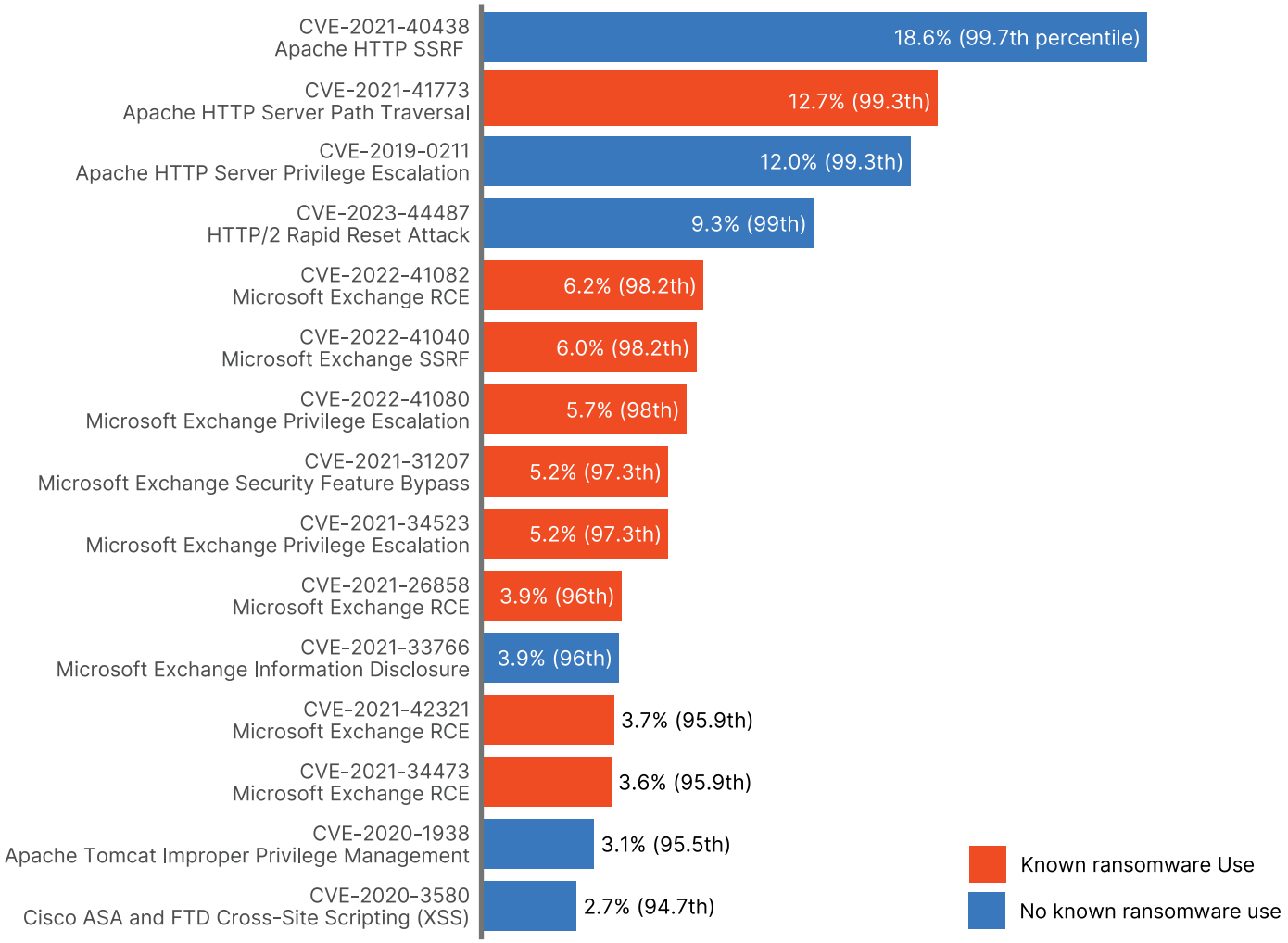
Cumulative distribution of average number of KEVs per week experienced by organizations. This chart shows the percentage of organizations that exceed a particular weekly rate. For example, 85% exceeded an average of 0.1 KEVs per week in 2023, 60% of organizations exceeded an average of 1 KEV per week, and about 2% of orgs exceeded an average of 10 KEVs per week.



What's interesting about ***Figure 6***, is that 60% of organizations experience more than one per week with a steep decline to ten a week, but there are a few that have dozens... and there are a few out there that average nearly 100 per week. That's a lot of exposure for some, and a little bit for others, but when we are talking about things that are detectable from the outside and are known to be actively exploited, a little bit of exposure can go a long way.

FIGURE 7: Top CVEs by percent of entities in 2023

In addition to the prevalence (% of organizations detecting that KEV in 2023), we also include the percentile of that prevalence among all CVEs that Bitsight detects. This means that the CVE-2021-40438 is at the "top of the class" and is more prevalent than 99.7% of other CVEs.



Now that we've investigated the magnitude of exposure for KEVs in a couple of different ways, let's get into the nitty gritty of what KEVs and where that exposure is concentrated. First, which KEVs did we find the most? Take a gander at ***Figure 7***.

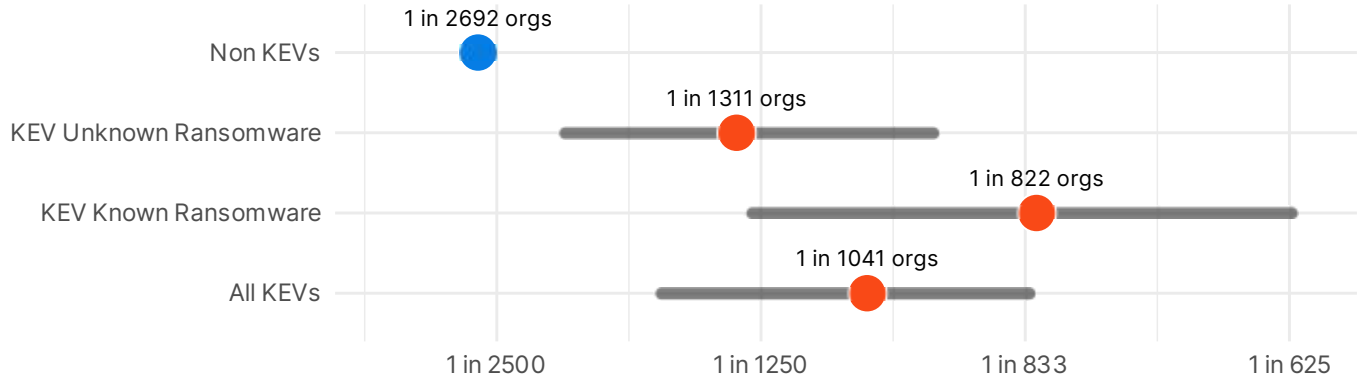
Given the nature of our view of the KEV catalog the results in ***Figure 7*** aren't terribly surprising. Apache HTTP Server is in widespread use, has frequently been the target of scary vulnerabilities, and because of its nature of *needing* to be externally facing to be useful at its job (serving web pages), it's unsurprising we detect vulnerable versions frequently. Microsoft Exchange servers having a relatively high prevalence everywhere is both surprising and not. It's surprising because we wonder about the wisdom of running an Exchange server open to the internet, but unsurprising, because we know it happens and we know there have been a large volume of vulnerabilities in Exchange servers.

But is the range we see in ***Figure 7*** (3%-20%) meaningfully high? After all, KEVs present a unique risk in that they are known to be exploited, but maybe that risk is ameliorated because they aren't as common as other vulnerabilities? If only. ***Figure 7*** dispels that wishful thinking.

What we see in ***Figure 8*** is that the median KEV is 2.6x more prevalent than non-KEV (found in ~ 1 in every 1k orgs for KEV vs 1 in every 2.7k for non-KEV vulns). This is again heavy-tailed, and as we saw in ***Figure 7***, some vulns have prevalence much higher than the median. The split between KEVs known to be used in ransomware, and those not known, is also stark with ransomware vulns being typically 64% more prevalent.

FIGURE 8: KEV vs Non-KEV median prevalence.

Error bars above represent the standard error of the median calculated through bootstrapping.



2.6x Median KEV is 2.6x more prevalent than non-KEV

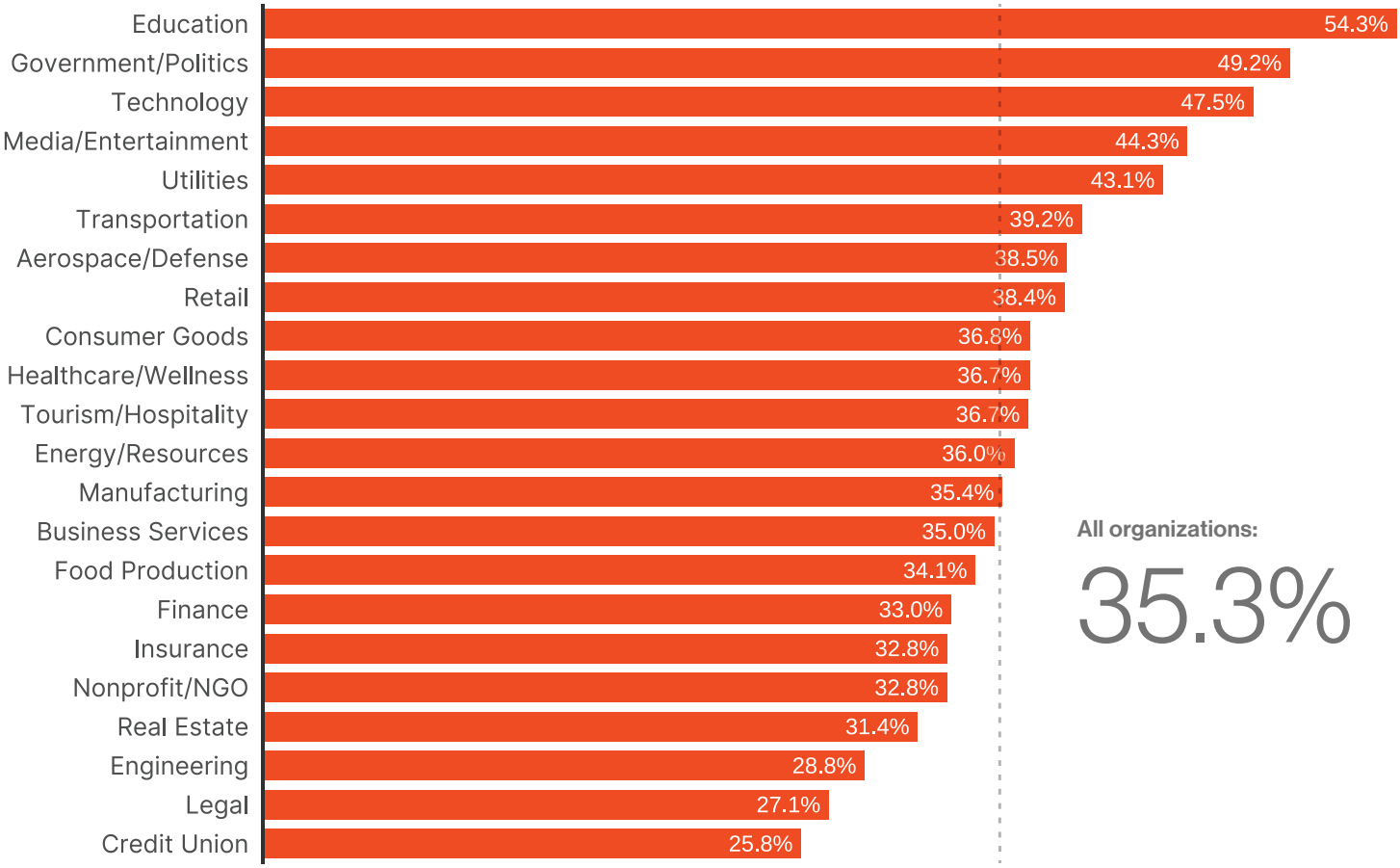
64% ransomware vulns are 64% more prevalent

Breaking Down Prevalence

So some KEVs are very common, and are typically higher prevalence than non-KEVs. But where is that prevalence concentrated? ***Figure 9*** starts us off by looking at different industries and where exposure is the highest.[9]

The variation here is pretty wide (though not by orders of magnitude) with some of the most likely players at the top of the list. In the above chart we remove service providers and cloud service providers. Education is another industry often stuck below the "security poverty line," meaning they are also at the top of the list. The same could be said for Government organizations which contain state and local governments as well as Federal. We'll get into whether US Federal Agencies do better with the KEV (as required) than others in a bit.

FIGURE 9: KEV prevalence by industry, 2003-2023



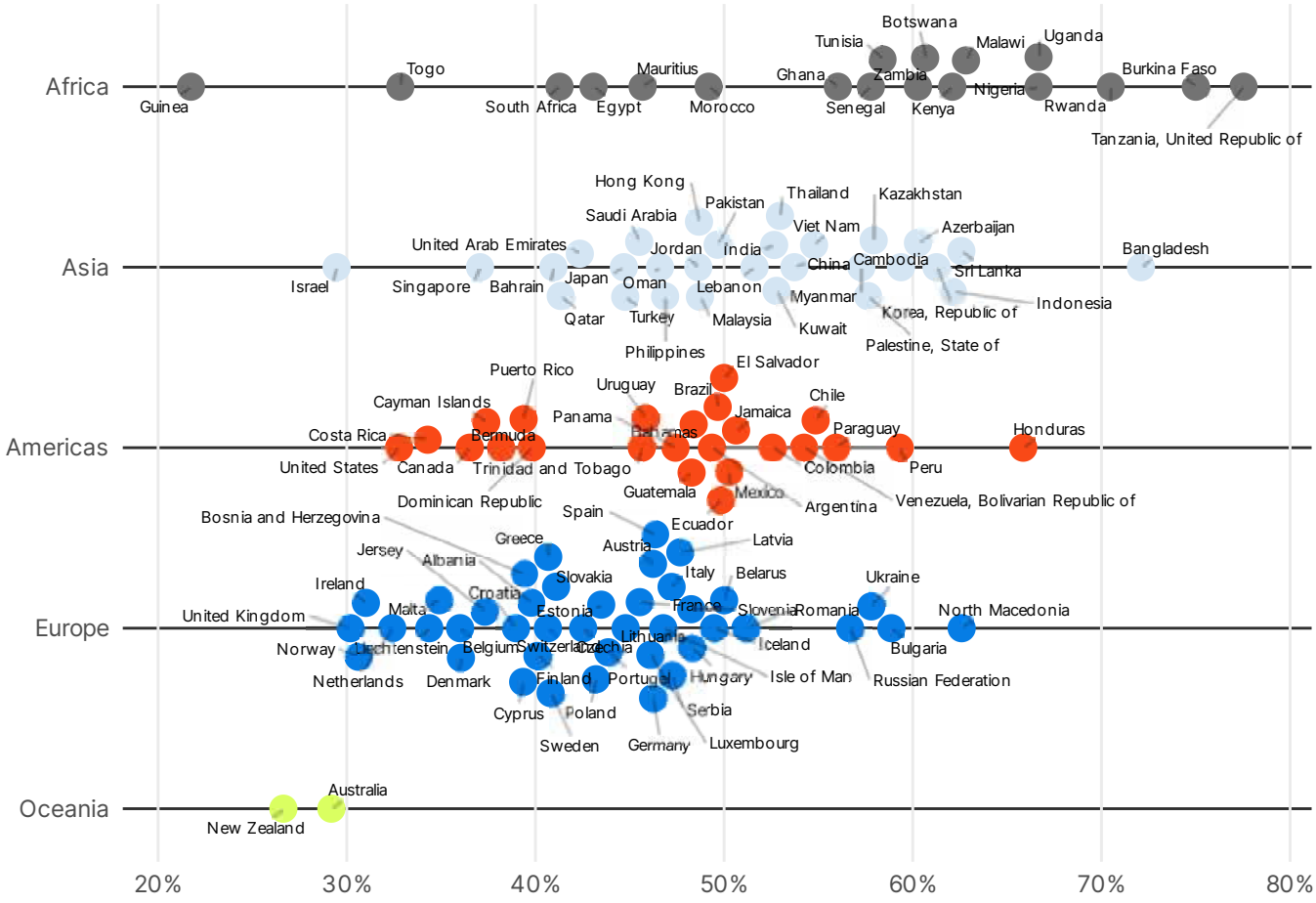
[7] For the next few results we are going to move back to our blunt instrument of "percent of orgs experiencing a KEV," as opposed to our more precise "average KEVs per week." We do this for two reasons: 1) at an aggregate level the two measures are highly correlated (see Appendix Figure A2 and A3), 2) it's a bit easier to communicate. That is, "X% of organizations in industry Y had a KEV in 2023" is more digestible than "Orgs in industry Y had an average of Z KEVs per week, on average."

The other major division of organizations that people tend to be interested in is geography. ***Figure 10*** takes a look by country.

We will note that ***Figure 10*** describes exposure only. Some may be surprised, for example, to see that a country like Germany — with a strong international reputation for cybersecurity — has an above average rate of KEV exposure and lies in the middle of the road for Europe. Further analysis will show that remediation rates vary dramatically by company and country, which we will explore later in the study.

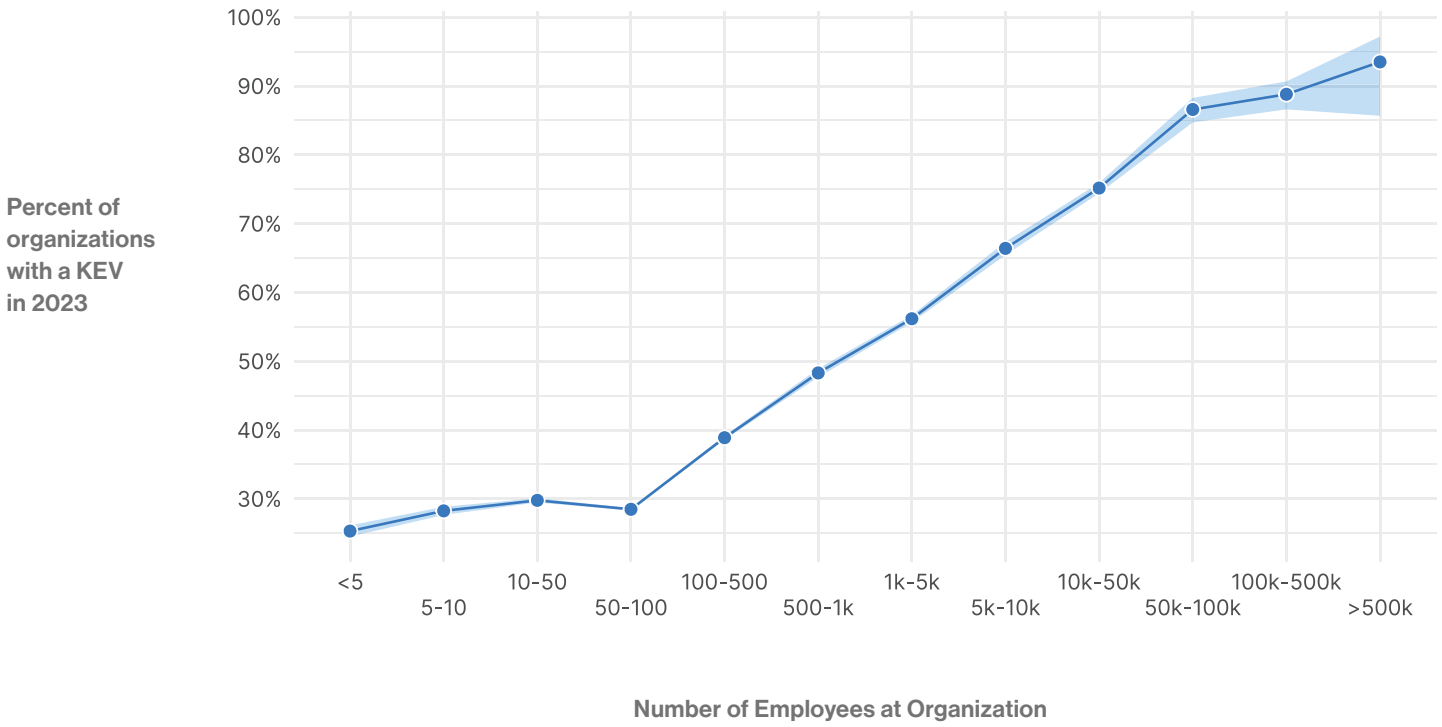
FIGURE 10: KEV prevalence by country

Each dot represents a single country with its location on the horizontal axis indicating the prevalence among organizations in that country. Circles avoid each other and stack when they have similar prevalence, helping show where a region's countries are most concentrated. We only show countries that we have sufficiently large samples to make a good estimate of the prevalence.



Indeed, this is a trend we see if we consider organizational size in ***Figure 11***. Larger organizations with their larger footprints simply have more chances to have a detectable KEV. Once we reach 50k employees or more, there is an 85% chance that organizations will have detectable KEVs. Again, this isn't an indictment of these large organizations' ability to address security issues, but rather a consequence of the complexity of their networks.

FIGURE 11: Organizational size and KEV prevalence



Unusual KEV Prevalence

Before describing how organizations react to KEVs in the next section we wanted to explore if there were any vulnerabilities that had particularly high concentration in any particular industry or country, and ***Figures 12 and 13*** explore that respectively.

FIGURE 12: Comparison of the prevalence of KEVs within industry (red) and with overall rate (gray)

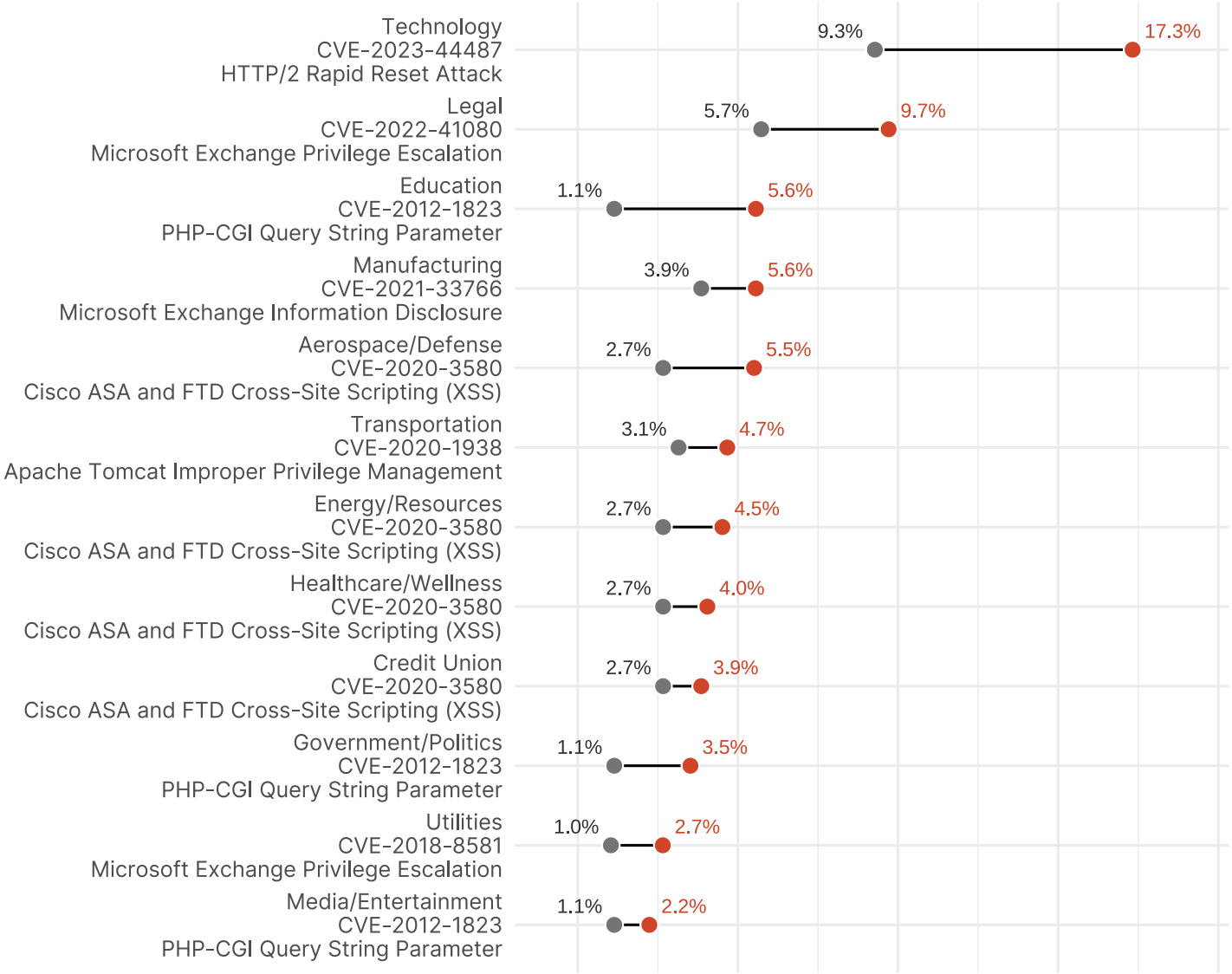
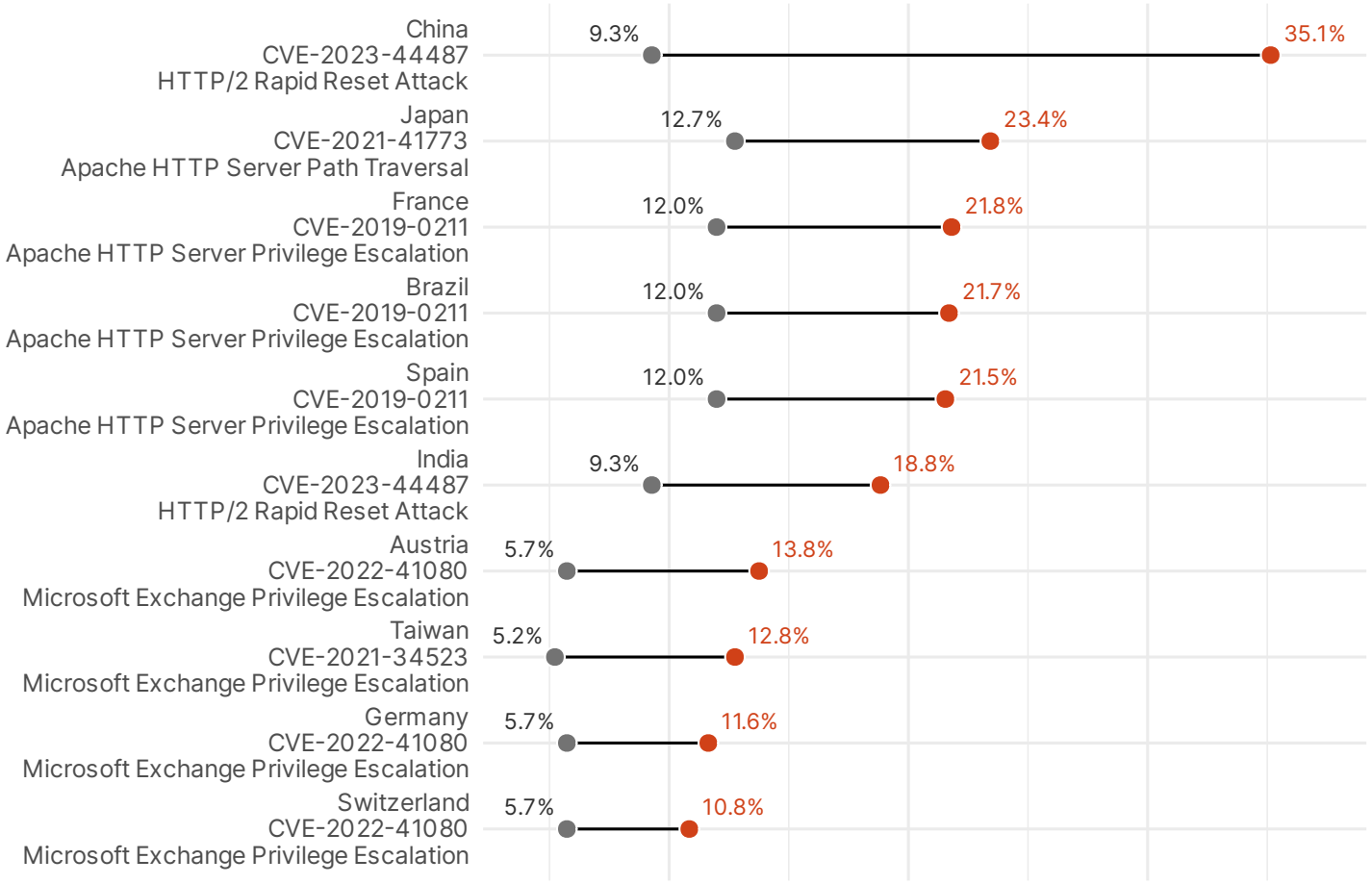


FIGURE 13: Comparison of the prevalence of KEVs within country (red) and with overall rate (gray)



Some vulnerabilities are much more common in certain industries and countries. These figures filter to vulnerabilities that affect more than 1% of organizations, and are at least 25% more likely in a particular industry or country than overall, again excluding service providers and cloud service providers. What's interesting here is that many of the same vulnerabilities that were extremely common (***Figure 6***) are even more concentrated in certain locales. There are some standouts, however, with Education having an extremely unusual concentration of the ancient CVE–2012-1823. This more than a decade old vulnerability affecting PHP installs has been long patched, but the concentration may represent a myriad of deployed and neglected infrastructure indicative of many an educational network.

But exposure is really only part of the battle. After all, many of these vulnerabilities are "surprises" in that they are zero or near zero days. In those cases exposure, especially for popular software, is going to be inevitable. It's what organizations do with that information that is important, and that's where we are going in the next section.

Getting Things Fixed

Tracking how quickly organizations react to new vulnerabilities can be a bit tricky. We'd like to know two things that tend to be correlated, but aren't always.

How long does it take for an organization to remediate a vulnerability after we detect it?

What percentage of vulnerabilities get closed by the CISA prescribed deadline?

An organization that has good security ideally does well in both. That is, they close a large percentage of the vulnerabilities they detect very quickly. But it's possible to be "good" in one but bad in the other. For example, an organization might have hundreds of vulnerabilities, and close a handful in just a few days, leaving the rest lingering. This is fast, but far from complete, remediation. Similarly you might have an organization that takes things slow and steady, fixing nearly everything, but taking months to do so. Both have their own inherent risks.

This is all complicated by the fact that we can't scan the entire internet for every CVE that Bitsight tracks in an instant. In fact, a full scan that collects the full depth of information that we could possibly collect often takes the better part of a day. Vulnerable assets we see at the beginning of the scan may be remediated by the end.

Luckily, this is a problem that exists outside of cybersecurity as well. In fact, a whole subfield of statistics is called "survival analysis" that seeks to quantify just that. Survival analysis was developed to track patient recovery (or, more morbidly, survival) after disease diagnosis. It centers on the idea that if we have a sample of patients we know are recovered, we can use the time it took them to recover to estimate the recovery of the patients in the study at any given time.

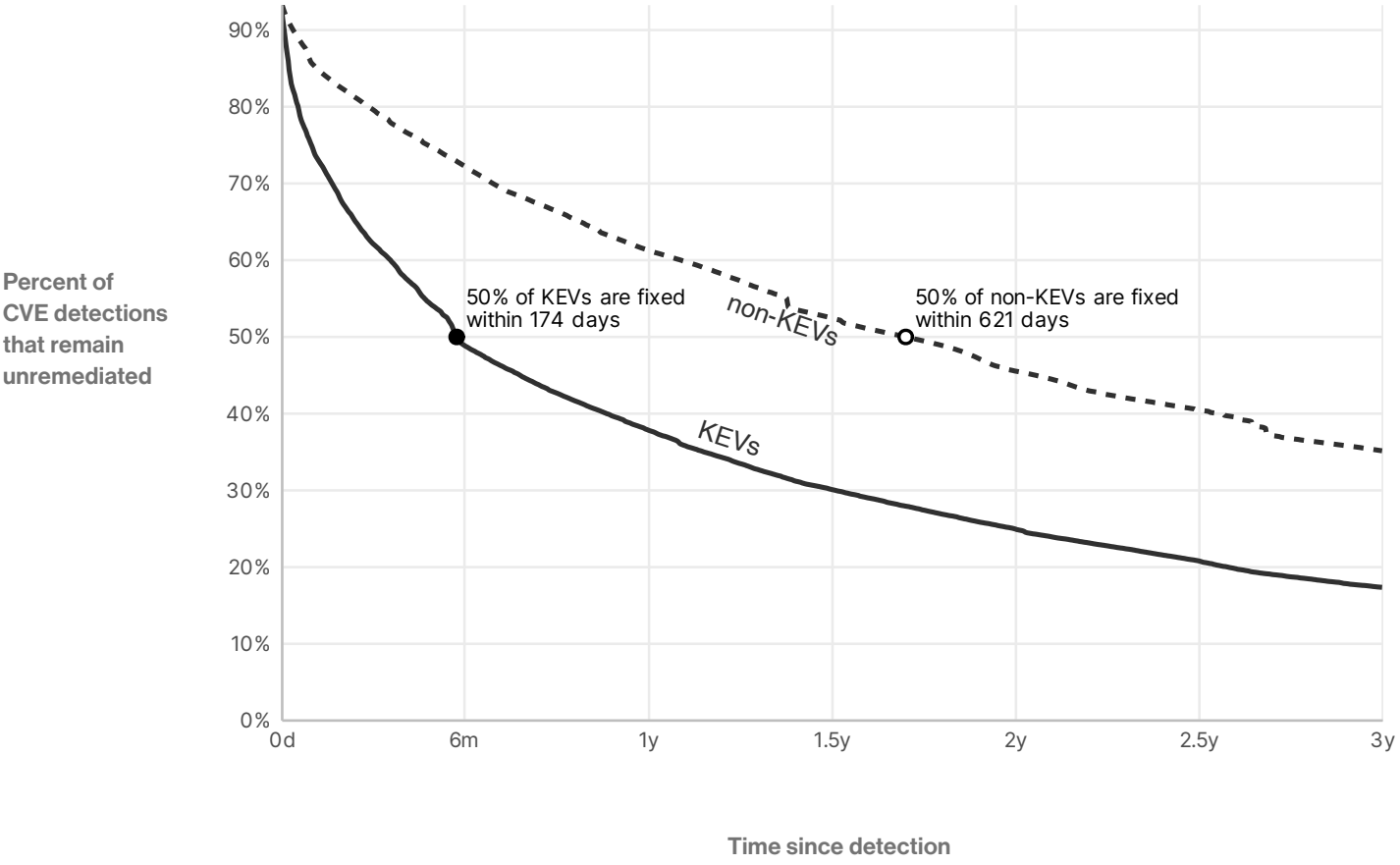
We can take this same approach to vulnerabilities. We mark when we first and last see when a particular organization was vulnerable to a KEV, and whether they had recovered the last time we measured. Because this is a robust and well developed set of methodologies, we integrate all sorts of interesting measurements.

Vulnerability Survival Time

The first question, and most obvious question is: do organizations remediate KEVs faster than vulnerabilities not in the KEV catalog? The answer is a clear "yes," which can be seen in ***Figure 14***.

What ***Figure 15*** shows is how long it takes a typical organization to remediate KEVs and non-KEVs. The steeper the descent of the curve indicates organizations are faster to fix those vulnerabilities that we scan. It's helpful to quantify those curves down to a single number and it's typical for survival analysis to ask what the time to remediate 50% of vulnerabilities. This 50% is the same as the "median time to remediation" and here it's a staggering 3.5x faster (174 days vs 621 days) to remediate KEV vulnerabilities.

FIGURE 14: Survival curves for KEV and vulnerabilities not on the KEV[10]



[10] *For those interested in the statistical details, these are computed using Kaplan-Meier estimates.*

But, while we do know that the selection process for the KEV doesn't explicitly include severity, there does seem to be a bias towards more severe vulnerabilities (measured by CVSS). Indeed, in our sample nearly 60% of KEVs as of this writing were CVSS Critical, compared to just 30% of non- KEVs (***Figure 15***).

If we break down the survival curves in ***Figure 14*** by severity, the reasons for the stark speed difference becomes apparent.

FIGURE 15: Survival curves for KEV and vulnerabilities not on the KEV

Distribution of KEVs and non-KEVs by severity. Note there are no KEVs that Bitsight tracks that are Low Severity.

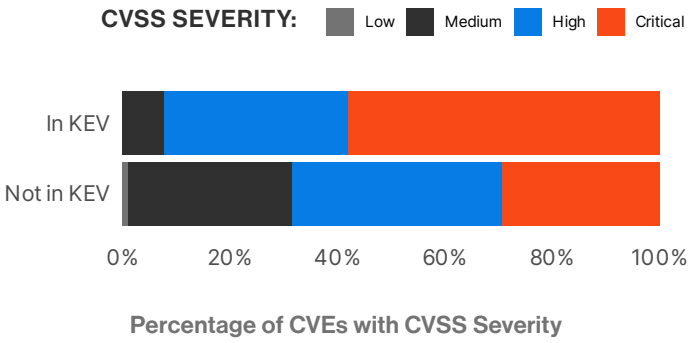
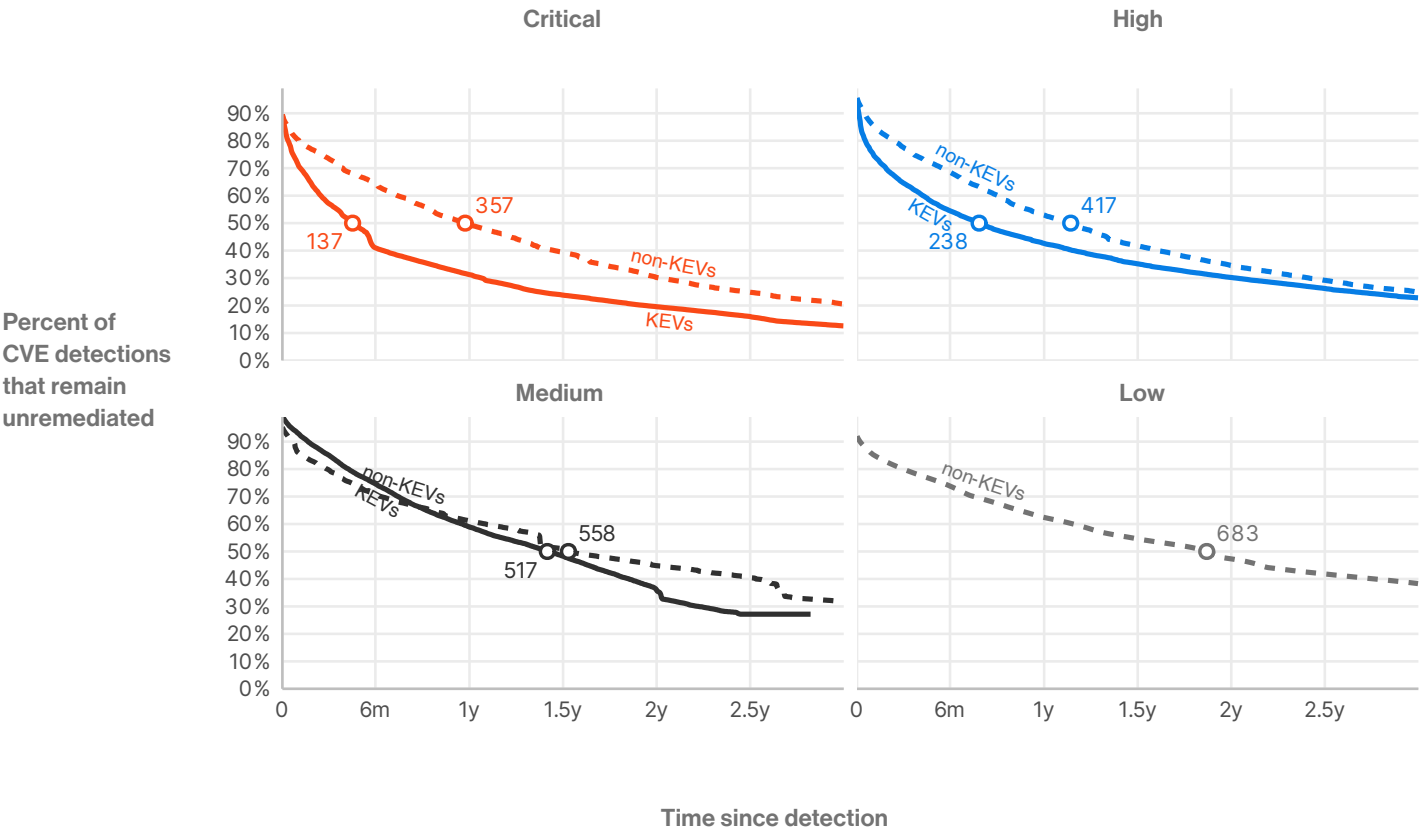


FIGURE 16: KEV survival curves by CVSS qualitative severity



Among Medium severity vulnerabilities, there is almost no difference in remediation speed. However, the median Critical KEV is remediated 2.6x faster than a non-KEV counterpart, with High severity KEVs remediated 1.8x faster than non-KEVs

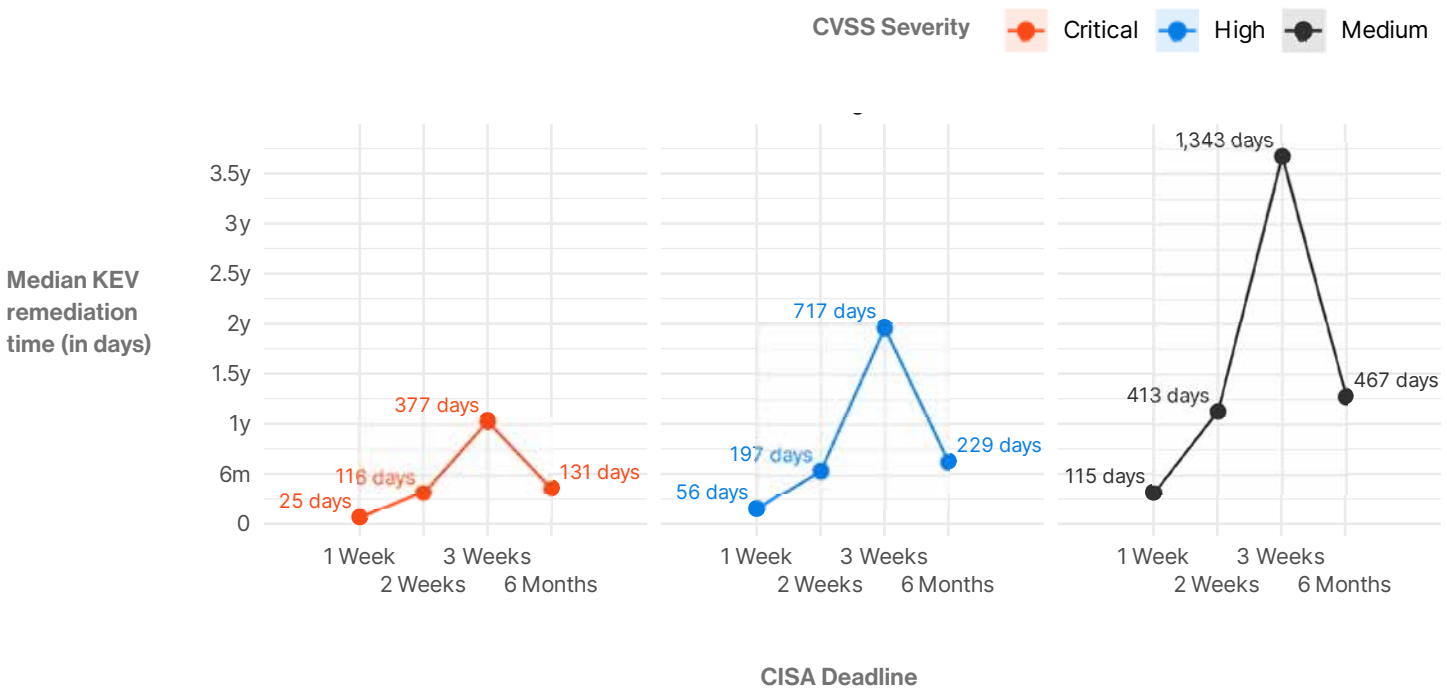
We've put survival curves in ***Figures 14 and 16*** on a 3 year scale, if we extend them out further we see further remediation, though not everything gets fixed. That doesn't necessarily mean the things left lingering are necessarily a large organizational risk. It's possible that those vulnerable systems need to remain in place for some reason or another, and that other mitigations are in place to ensure they don't cause damage to the organization.

As we mentioned when we discussed the KEV catalog, in the introduction, the catalog provides additional information besides "this vulnerability is being exploited." In particular, they give a deadline for how long after a vulnerability is added to the KEV catalog that U.S. federal agencies have to do whatever CISA recommends to remediate things. This gives us a sense that those vulnerabilities with shorter deadlines likely should be fixed faster, but are they? ***Figure 17*** indicates "mostly."

In ***Figure 17***, we collapse those full survival curves from ***Figures 14 and 16*** down to the single value we annotated, the median time to remediation. The general trend here confirms "more severe are fixed faster" and "shorter deadlines get fixed faster." We'd note that the median time is in nearly all cases much longer than the deadline, implying that more than half of KEVs do not get fixed by the prescribed deadline. We'll get into the likelihood of meeting the deadline a little bit later on.

The other thing that stands out in ***Figure 17*** is the fact that the 6 month deadline vulns break the monotonicity we might expect. This is largely due to the fact that the vulns with a 6 month deadline in the data above were largely older vulnerabilities that were part of the KEV catalog when it was initiated. In particular those with a 6 month deadline were typically (median) published ~2.5 years before their addition to the KEV catalog, compared to 6, 3, and 10 months for the 1, 2 and 3 week deadlines respectively.[11] This means that for many 6 month deadlines patches were widely available and any regular update would fix these vulnerabilities, likely leading to their quicker remediation.

FIGURE 17: Median time to remediation by CISA deadline and CVSS Severity



[11] *See Figure A4.*

Next, we want to see how remediation rates correlation with known ransomware use. Certainly ransomware presents a clear and present danger for organizations, so we'd hope that organizations manage to fix ransomware KEVs faster than non ransomware KEVs (***Figure 18***).

Figure 18. KEVs known to be used in ransomware remediation time vs those not to be used in ransomware. This speed-up in the face of digital extortion is really what we'd like to see given the threat it poses. If we average out the relative drops, ransomware KEVs are fixed 2.5x faster (on average) than KEVs not known to be used in ransomware. In fact, it's helpful to see just how this speed manifests itself in ***Figure 19***.

FIGURE 18: KEVs known to be used in ransomware remediation time vs those not to be used in ransomware

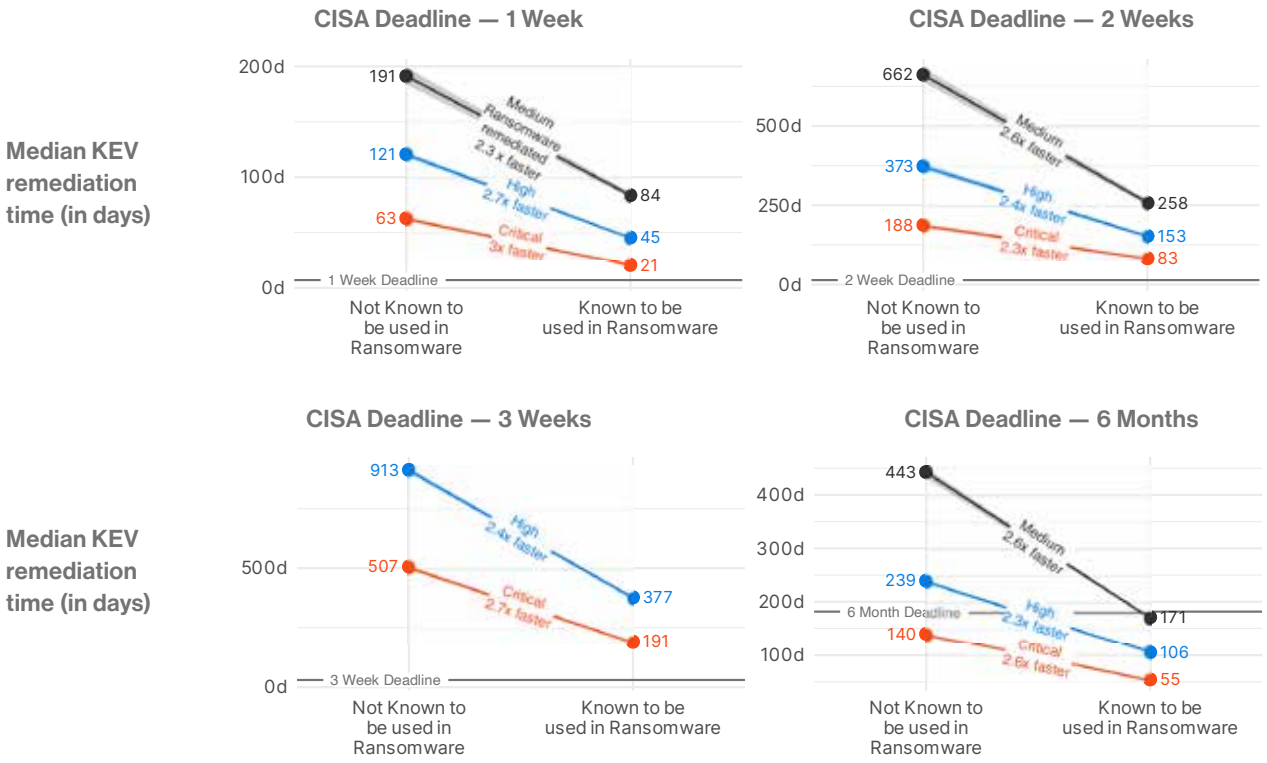
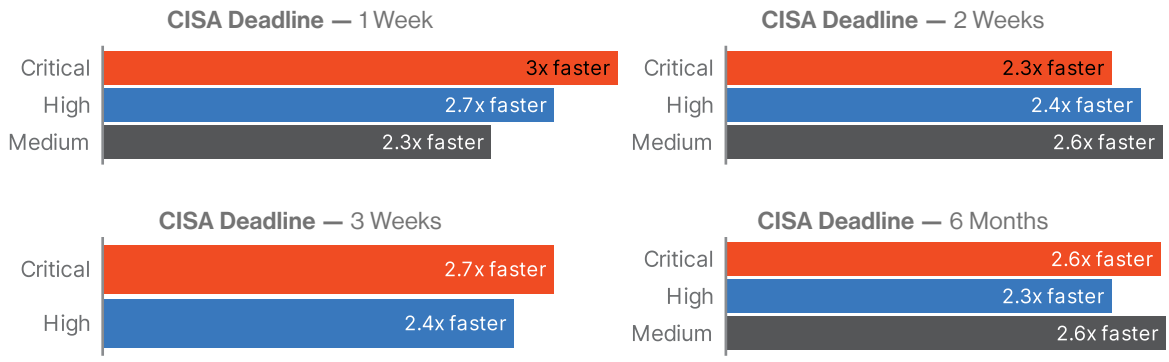


FIGURE 19: Change in median time to remediation between Ransomware and non-Ransomware KEVs

Change in median time to remediation between KEVs known to be used in Ransomware and those not known to be used in Ransomware.



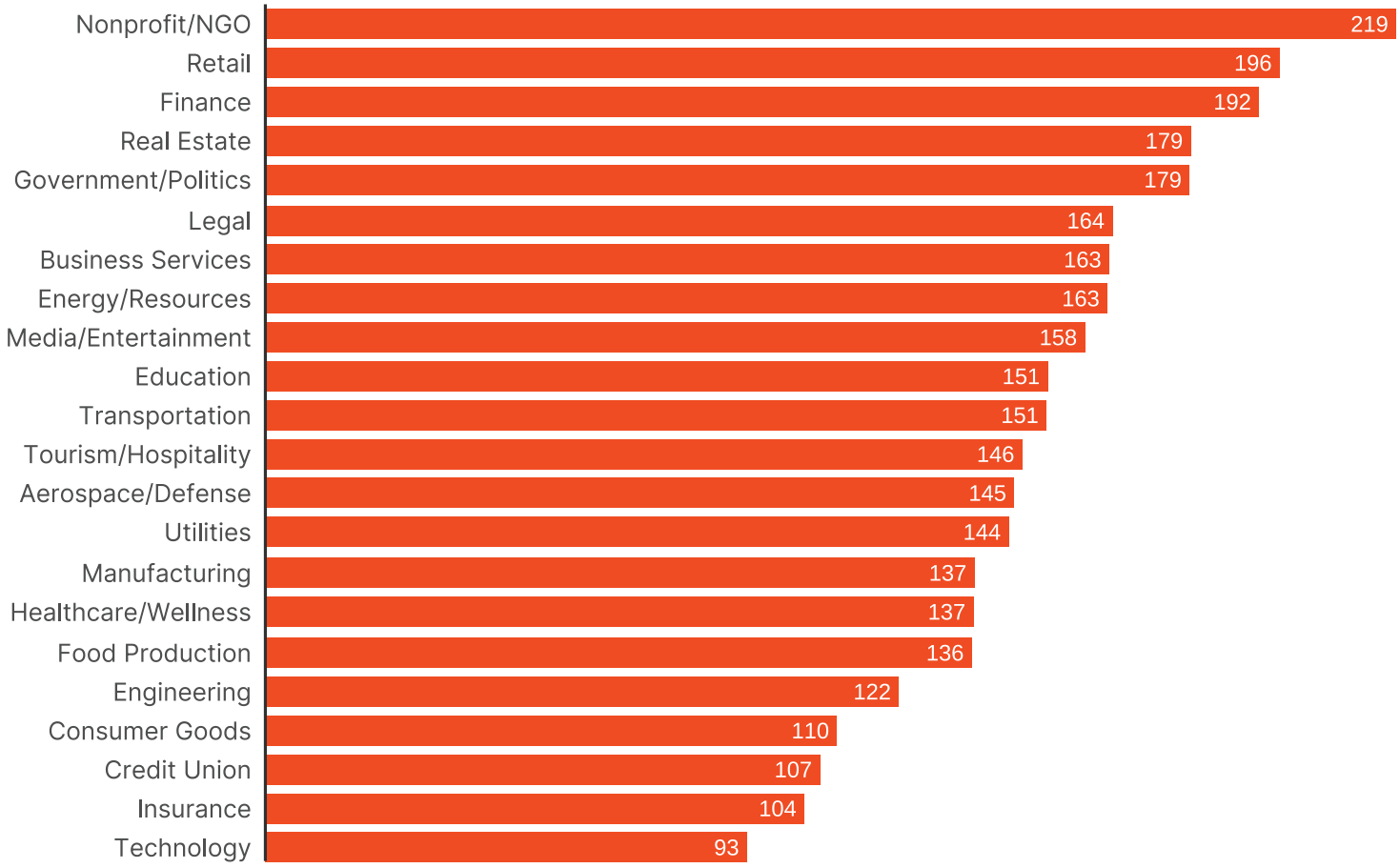
Change speed of remediation between ransomware and non-ransomeware KEVs

It's now worthwhile to start breaking down which types of organizations manage to remediate KEVs most rapidly, and do some comparative analysis to their exposure. First, let's look by industry.

Figure 20 offers both contrast and similarity to ***Figure 9***. In particular, we see that Technology organizations are some of the fastest to remediate vulnerabilities whereas they are near the top in terms of exposure. However, Nonprofits and Governments are near the top of both lists, making them uniquely at risk from KEVs.

One thing we'd draw the reader's attention to is that ***Figure 20*** averages over all the things we found to be important over the previous few results. We'll take a quick detour away from the simplicity of the bar chart in ***Figure 21*** to a chart where we try to display four different quantities at the same time.

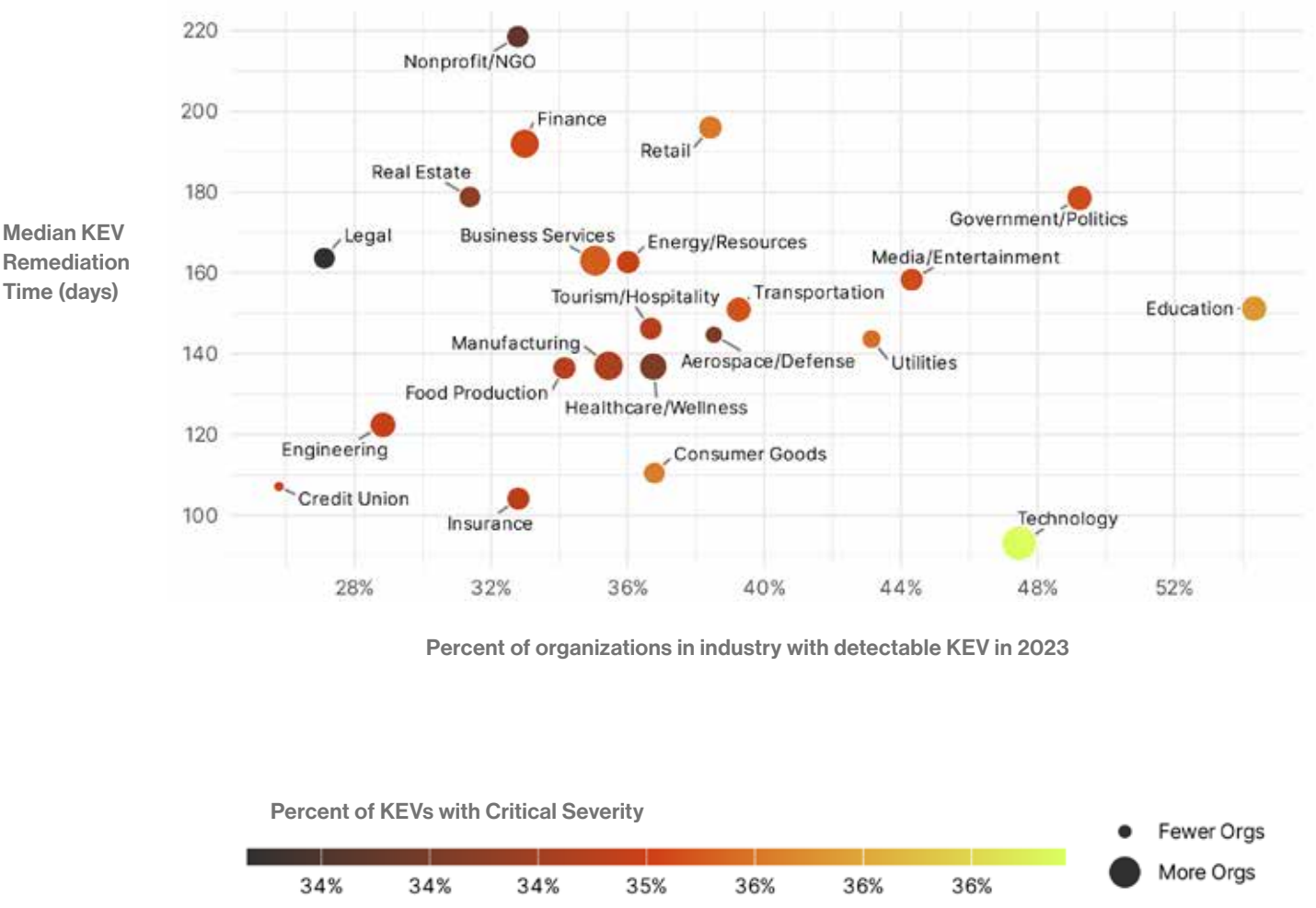
FIGURE 20: Median KEV remediation time (days) by industry



What ***Figure 21*** shows us is that Technology manages to remediate quickly. This is a good thing as they are also the highest exposure industry, 3rd most likely to experience a KEV in 2023, and with high proportions of Critical KEVs. The place we don't want to see organization is in the upper right, high exposure and slow remediation, where Education and Government/Politics are. Where you do want to be is the lower left, with Insurance, Credit Unions, and Engineering organizations. These have relatively low exposure and low rates of critical severity KEVs *and* they fix things quickly.

FIGURE 21: Remediation and exposure across industry

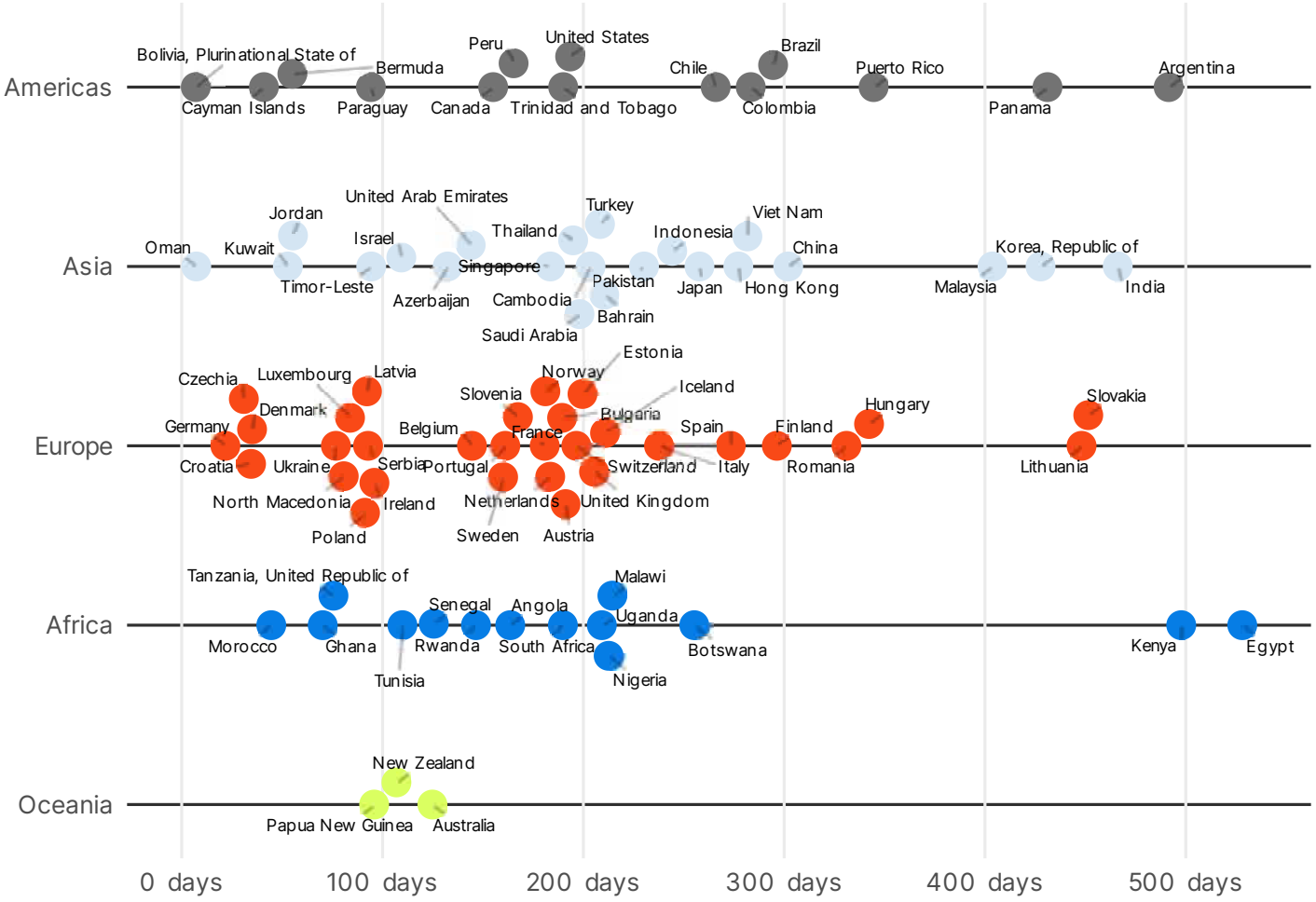
The color indicates the percentage of CVEs detected by organizations that are critical, and the size is scaled to the number of organizations in that industry.



Next, let's turn our attention to the globe and see what is happening with remediation on a country level in ***Figure 22***.

Here, we contrast with the data in ***Figure 10***. We'll let folks generally choose their own adventure here, but there are a few interesting standouts once again. Germany, with its relatively high exposure, ends up the fastest in Europe in getting things cleaned up. The UK, in contrast, is relatively slow on remediation, even with its relatively low exposure.

FIGURE 22: Country level median remediation times



Before we move onto another interesting measure of remediation, we are going to revisit the last firmographic measure: organizational size.

In ***Figure 23***, we see the opposite relationship we saw in ***Figure 11*** across the board. The more employees an organization has the faster things get fixed. This is likely due to those larger organizations having the maturity to have visibility of assets and a clear plan of action for fixing vulnerabilities.

FIGURE 23: Median KEV remediation time and organizational size.

Meeting the Deadline

As we mentioned at the outset, the KEV catalog provides a useful bit of guidance by giving U.S. federal agencies a specific deadline for which they'll need to remediate KEV vulnerabilities. Since we've got those remediation curves, we can actually ask how frequently each of those deadlines is met for the CVEs in our dataset (***Figure 23***).

We can make two interesting observations in the data in ***Figure 24***. First, there are a full 16 vulnerabilities that are *never* fixed by the deadline in our data: 9 with a 6 month deadline, 4 with a 3 week deadline, and 3 with a 2 week deadline. That's not to say that these never get fixed by the deadline by anyone, but in our data they never do (we'll talk about which ones they are in a bit). The second interesting thing is that there is quite the spread no matter what the deadline is or whether it's used in Ransomware. In the next figure, we'll find that, on average, some deadlines are met more than others, but the variation among CVEs is pretty large no matter what.

The KEV catalog provides a binding deadline only for U.S. federal agencies. Are U.S. federal agencies better at remediating KEVs compared to all other organizations?

FIGURE 24: Percent of instances of KEVs that are remediated by their given deadline

Each point is a KEV, placed on the horizontal axis at the calculated percentage.

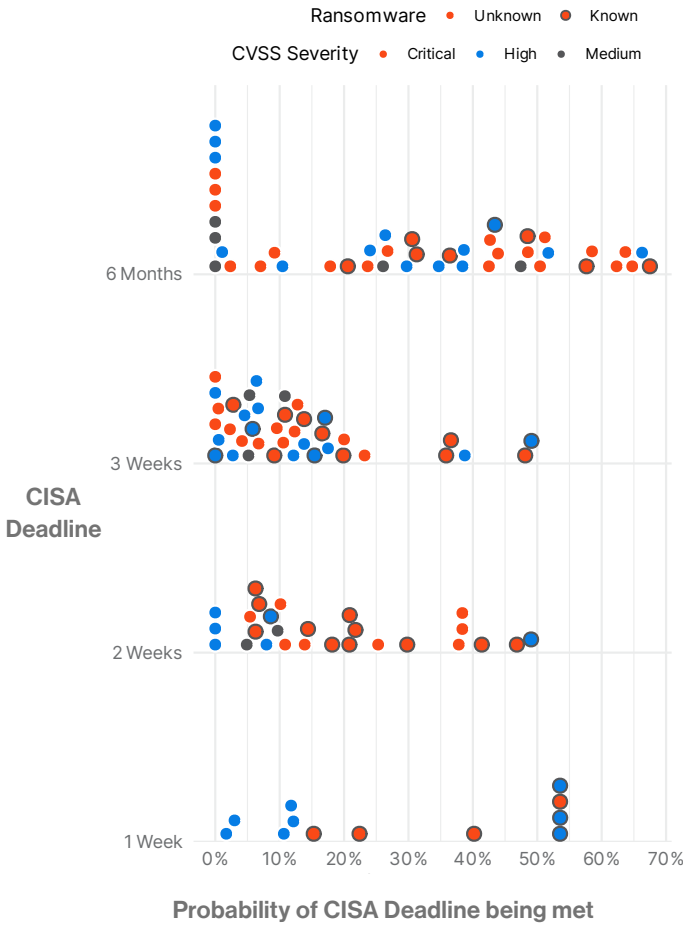
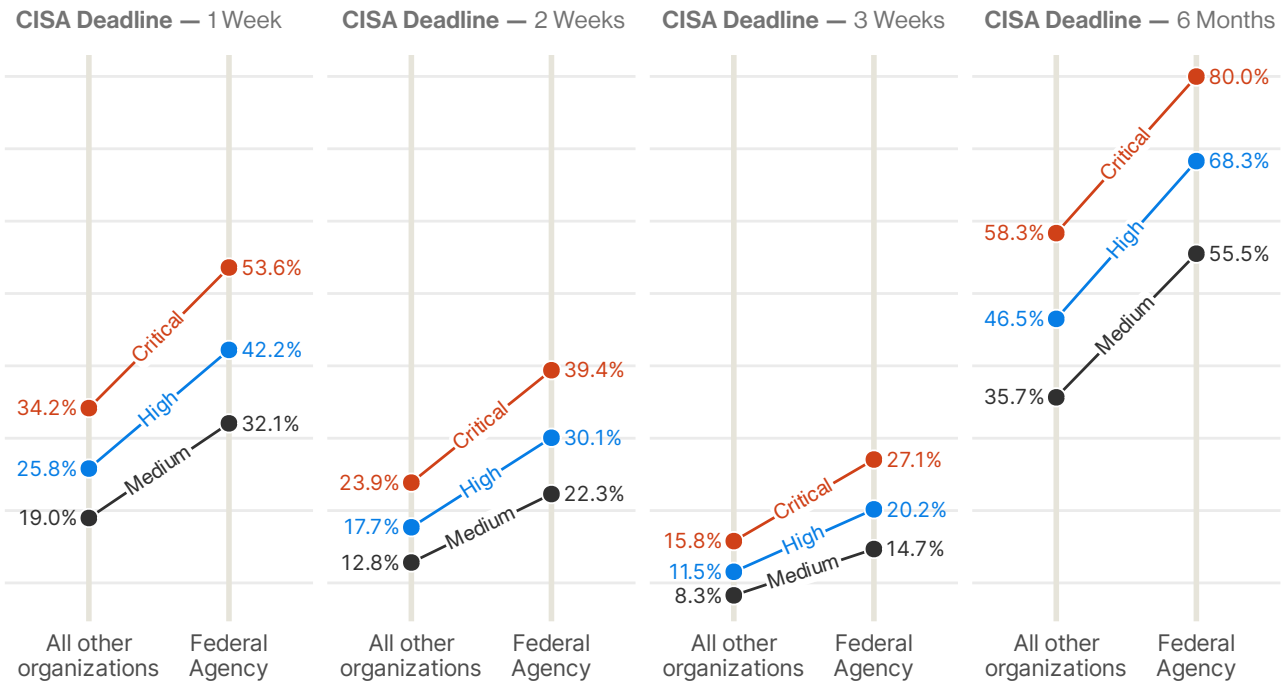


FIGURE 25: Probability of KEVs fixed by the CISA deadline for federal agencies vs all other organizations.



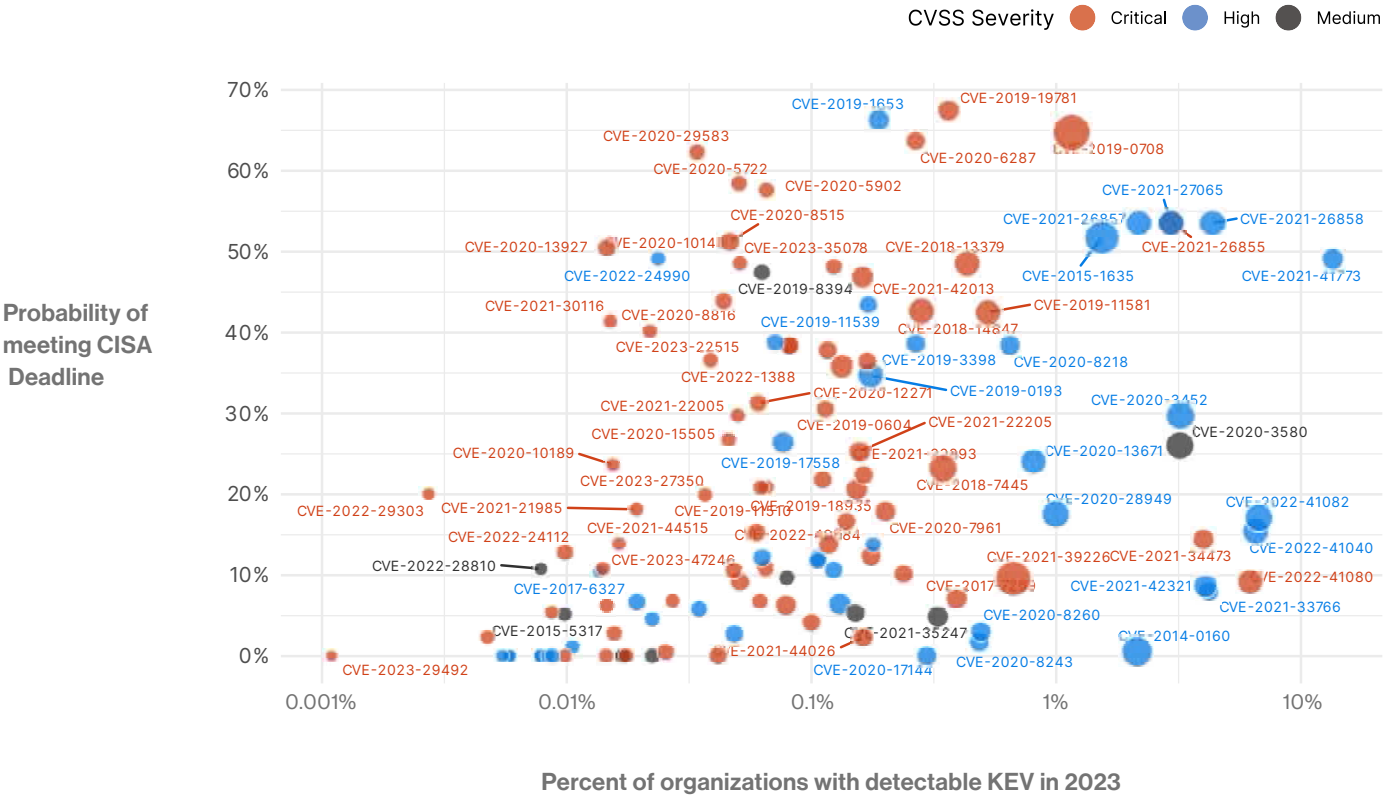
While U.S. federal agencies are not perfect, they do have a marked improvement over everyone else in fixing things by the deadline. In fact, on average U.S. federal agencies fix 63% more KEVs by the deadline than everyone else.[12] This seems at odds with the slow pace of remediation seen in ***Figure 19*** for "Government / Politics," however, that particular industry sector includes both federal agencies as well as state and local governments, who apparently are a bit slower at remediation. If we weight the results above by how many times we discovered individual vulns, we find that 40% of KEVs are fixed by the deadline.

As one last piece of analysis we'll examine exactly which KEVs get fixed by the deadline compared to their exposure in ***Figure 26***.

[12] *This is the relative ratio, e.g. for 1 Week deadline critical vulns (53.6%-34.2%)/34.2% = 56%. The absolute difference is ~15% on average.*

FIGURE 26: Percentage of KEVs fixed by deadline and overall exposure of that KEV

The points are sized by "total detections" which may include multiple detections at the same organization or multiple detections over time. The absolute numbers aren't all that informative, but they give us a sense of how common these things are.



Again, ***Figure 26*** shows no strong correlation, though there is a statistically significant relationship with an increase in prevalence leading to a higher likelihood of remediation by the given deadline, but far from certainty. There are a few standouts however. CVE-2022-41080, a "critical" vulnerability in Microsoft Exchange servers, is rarely fixed on time, but affects a (relatively) high 6% of organizations.

As we mentioned above, there are 16 vulns that are never fixed by the deadline (represented by every point along the bottom of the figure). Don't be fooled by Heartbleed (CVE-2014-0160), which sits just above the line getting fixed by the deadline just 0.44% of the time. Unsurprising, given the vulnerability's age; if it hasn't been fixed yet, it's probably unlikely that instances are going to be fixed anytime soon. The highest prevalence vulnerability that *never* has been fixed by the deadline in our data is CVE-2020-17144, a Microsoft Exchange vulnerability that we found in about one in 341 organizations in 2023. At first blush, this might seem odd, given that patches are readily available, but this is more a complexity in data collection. Bitsight didn't support detections of this vuln until September of 2023. So like Heartbleed, the lingering detections are likely the "long tail" of forgotten vulns that may never be fixed.[13] Speaking of Microsoft Exchange, perhaps most concerning is CVE-2022-41080, found in roughly 6% of organizations, and only fixed by the deadline (3 Weeks) only ~9% of the time. In contrast, something with relatively high prevalence CVE-2019-0708, ie BlueKeep was found in more than 1% of organizations (and many individual detections!) is fixed by the deadline more than 60% of the time.

[13] *There is a lot of cross correlation in the data that affects how quickly Bitsight is able to detect vulns and how quickly folks remediate them. Folks remediate Critical and short deadline vulns faster and Bitsight manages to support them more quickly to help customers assess risk. When we dug in and included this in some of the models used to get the figures above, we found there remains some correlation between support and likelihood of meeting a deadline, but it is dwarfed by the effect of the severity, the deadline set by CISA, and whether it's known to be used in ransomware.*

Conclusions & Recommendations for Security Leaders

We've provided a whirlwind tour of the KEV catalog, slicing and dicing it in the most obvious ways. Bitsight data offers a unique view that allows for global analysis by sector and industry.

The kind of actionable intelligence the KEV catalog provides is crucial to any organization defending themselves. It's not just knowing "this is being exploited," but how it's being used by attackers, and even guidance for when things should be fixed. While the deadline given by CISA only applies to U.S. federal agencies, it is excellent guidance for any organization.

This study exposes some uncomfortable truths about the current state of vulnerability management. While it is common knowledge that vulnerability management and remediation is critical to the health, quality, and security of digital businesses, why do so many organizations continue to struggle? Experts we spoke with were unsurprised by our findings and point out that organizations struggle with vulnerability management because they lack:

Clear responsibility and authority for IT and Cybersecurity teams when it comes to vulnerability remediation. For example, although Cybersecurity teams are often in charge of identifying vulnerabilities within the organization's environment, they are dependent on IT teams to patch systems. This can impact remediation rates.

Visibility across their environment to know their vulnerability exposure. Organizations often lack tools that would provide visibility into vulnerability exposure within their own infrastructure and across their supply chain.

Metrics to ensure that IT and Cybersecurity teams are achieving the goals of the vulnerability management program. Metrics help create accountability for the program.

Conclusions & Recommendations for Security Leaders

Achieving success in vulnerability management requires leadership, process, technology, and accountability. Experts suggest that organizations have the following in place:

- **Corporate level strategy for vulnerability management.** This strategy should have executive-level support, set clear responsibilities for vulnerability management across the organization, define enforcement authorities and processes, and provide authority to Cybersecurity teams to patch at-risk systems.

- **Clear remediation timeframes based on vulnerability severity and business criticality.** Organizations should establish timeframes for Low, Medium, High, Critical, and KEV vulnerabilities. Typical patching rates range from 7 days (for Critical or KEV) to 180 days (for Low). Organizations should also consider emergency procedures for zero-day vulnerabilities. It's important to build a remediation plan that includes patching as a primary means for reducing risk but security teams should also include other mitigations in their plans, especially for use when addressing vulnerabilities that do not yet have a reliable vendor patch available.

- **Technology and automation to assess and remediate vulnerable systems.** Organizations need automated scanning capabilities to identify vulnerable systems on their own internal and external facing assets, along with their external supply chain and third party ecosystem. Organizations should be able to issue automated notices and work orders to owners, track remediation rates, and escalate issues when necessary. For Critical and KEV, organizations should have an automated process to enforce remediation, removing applications and devices from the environment after time frames and grace periods have been exceeded.

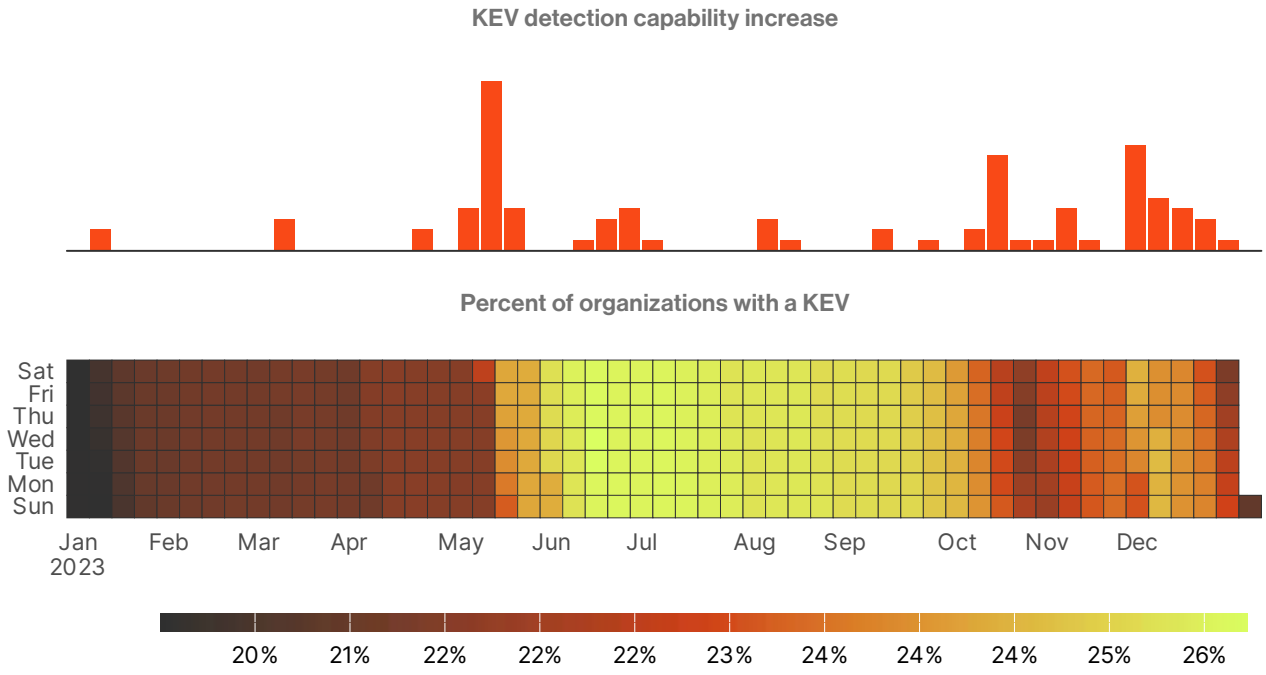
- **Metrics and accountability for the organization.** Metrics on remediation rates and vulnerable systems should be a critical part of business and executive reporting. These metrics should be available by organization, technology owner, and business leader. Metrics should be part of executive resilience and operational discussions. Patching and hygiene management objectives should be added to technology and business leader compensation. Metrics should be produced regularly and available continuously, show trends, and clearly provide several key insights to security leaders and executive management:

  - Whether agreed service level objectives for remediation are being met and whether the organization is accumulating a backlog of "remediation debt."
  - The mix of patching vs. mitigation to remediate issues. Mitigations may include removing vulnerable systems from service or leveraging third-party security tools to block exploits. Patching is preferred when possible.
  - The trend of technology debt at the organization in order to illustrate the accumulated growth of end-of-life systems–software that can no longer be patched because a vendor has stopped supporting it.

Appendix

The appendix is placed here to justify some of the assertions we made above, but including that justification would disrupt the flow of the report. First, we examine how Bitsight's capabilities and the growth of the KEV changed the daily detection rate over the course of 2023. **Figure A1** gives some details.

FIGURE A1: Daily rate of organizations with KEVs over the course of 2023.



Obviously, as the KEV catalog grew and Bitsight increased its detection capability (*top bar chart in* ***Figure 3***) the percentage of orgs with those detected CVEs decreased, with a slow decline as things get remediated (more on remediation later).

Next, we examined whether "Percent of organizations experiencing a KEV in 2023" was a good proxy for "Average number of weekly KEVs experienced by entities within a group in 2023, on average" (*See footnote*[5]).

Figure A2 and A3, show a strong correlation between the two measures at an aggregate level. We use the simpler, blunter measure because it is easier to communicate than the more complex, more precise measure given this strong correlation.

FIGURE A2: Correlation between measures of prevalence at a country level.

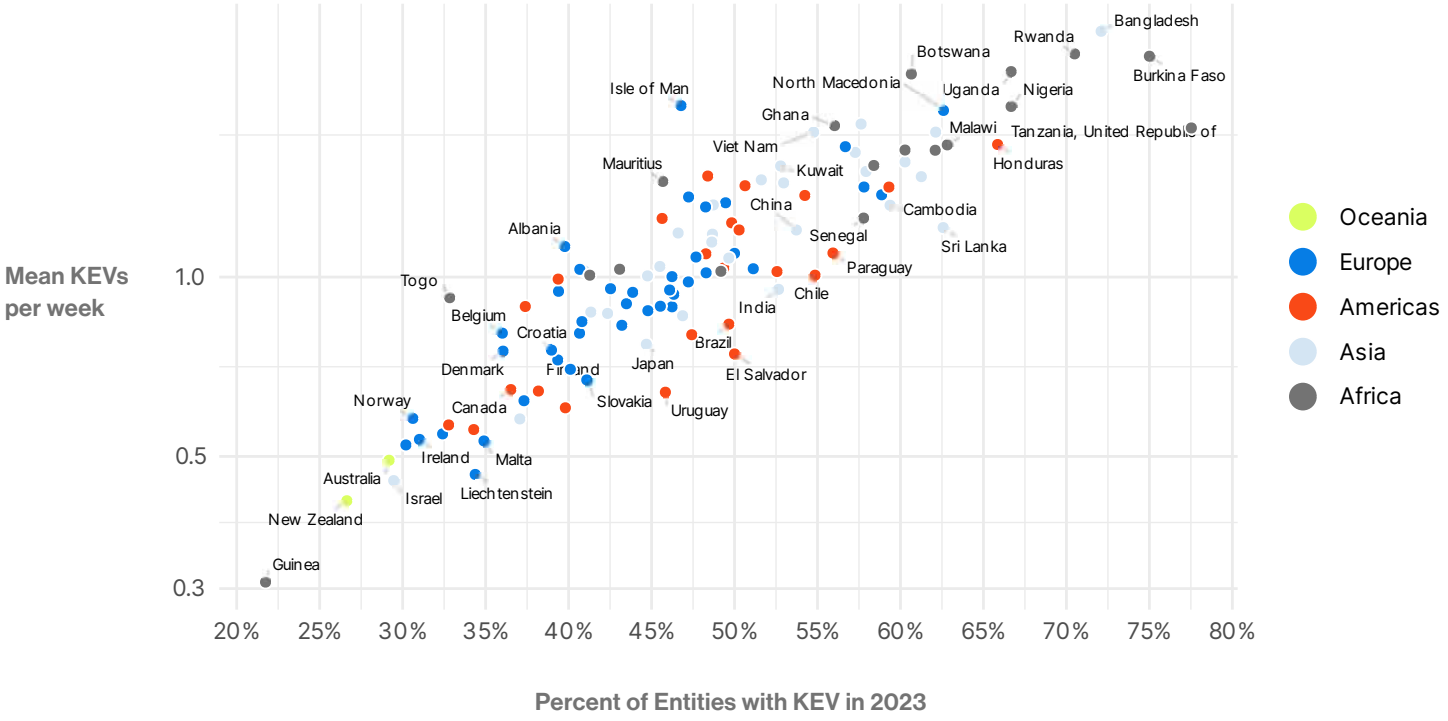
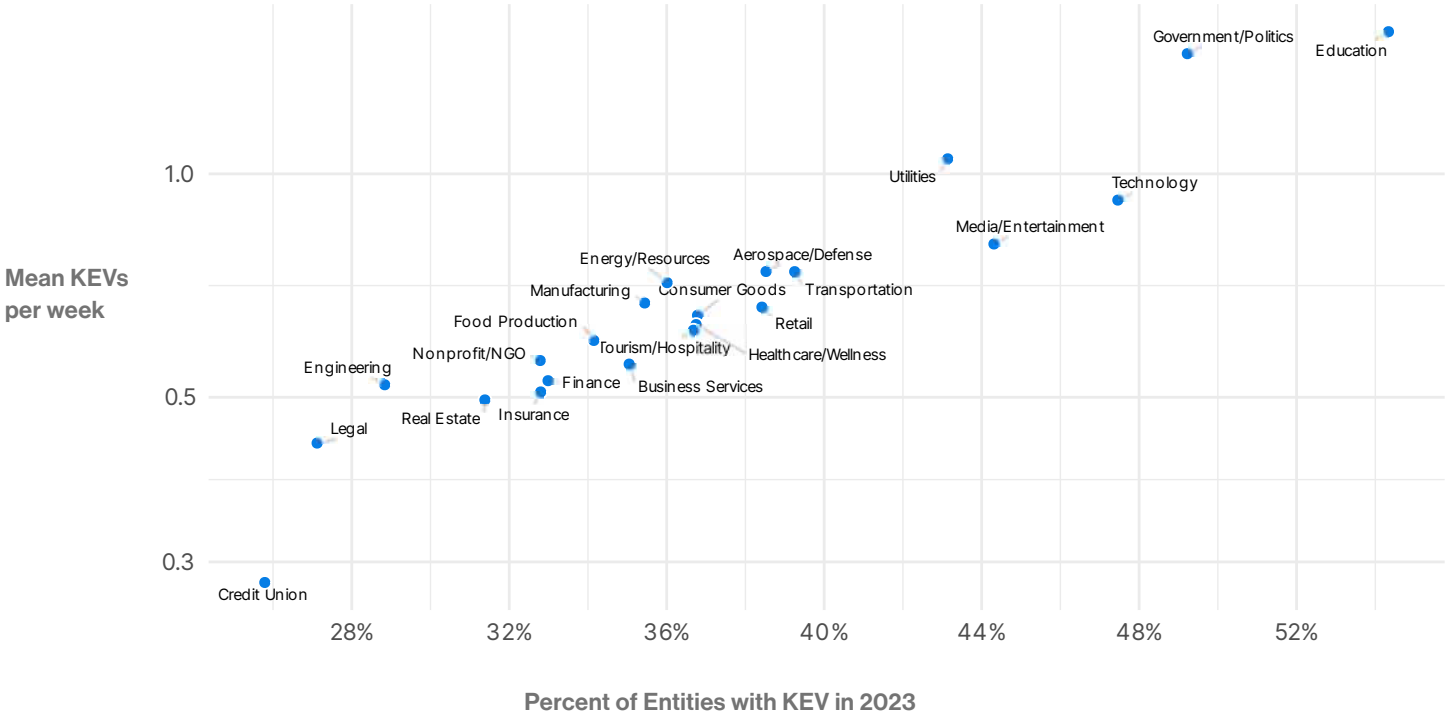
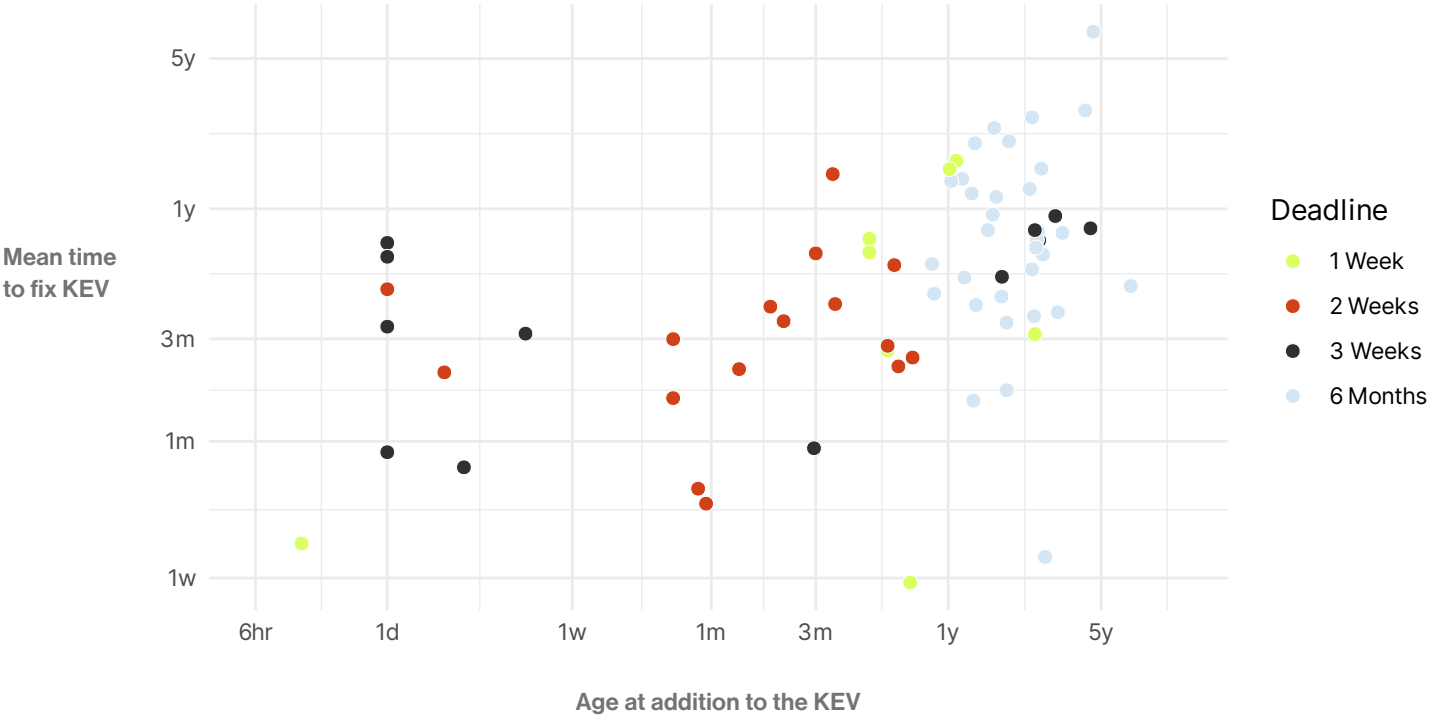


FIGURE A3: Correlation of measures of prevalence at an industry level.



Next, we wanted to examine the age when vulnerabilities were added to the KEV catalog. We extracted the publication date from the NVD catalog and compared it to when it was added to the KEV catalog. We note here that 6 month deadline vulns typically are much older than others, though there is quite a bit of variation.

FIGURE A4: Age at addition to the KEV vs remediation time.



Materials and Methods

For this study, we examined vulnerability detections at organizations over the course of 2023. We reviewed the security posture of 1.4m entities. For an organization to be included in the study, they needed to be scannable by our vulnerability detection capabilities, be active during 2023 (i.e. still operating), and not be a service provider or cloud service provider. All prevalence calculations were based on this sample of organizations within Bitsight data.

Bitsight only scans for the presence of a subset of vulnerabilities. These vulnerabilities need to meet several criteria. First, they need to be externally detectable, which excludes vulnerabilities that require local network or physical access to the asset, and also most client software vulnerabilities as they are rarely Internet facing. Second, a vulnerability needs to be detectable without actively exploiting the vulnerability. Bitsight strives to scan for vulnerabilities in a non-intrusive manner. Finally, it needs to present enough of a risk that it is worth the resources to discover. Capabilities during the course of this study include 7,772 CVEs of those 195 are listed in the KEV Catalog.

Prevalence calculations are only reported when we can be reasonably certain of their value. For each subset of data we calculate a 95% confidence interval for binomial data using a Wilson correction. If the width of the interval is greater than 0.25, we do not report that value. Median standard errors in ***Figure 8*** were calculated using bootstrap sampling with 5,000 samples.

Median remediation time, and whether remediation was completed by the deadline were calculated using Kaplan-Meier or Cox proportional hazard model estimates. All stated differences are statistically significant at the $p < 0.01$ level.

Acknowledgements

Dr. Benjamin Edwards is a principal research scientist working at Bitsight. An expert in ML and statistics, Ben synthesized security data into actionable insights. He has led research on a wide variety of security topics including vulnerability management, application security, human risk, Next-gen SIEM, nation state cybersecurity policy, and the security of ML models. He is an active member of the security community, contributing to open standards efforts including both EPSS and CVSSv4. His work has been published in leading industry and academic venues.

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.

BOSTON (HQ) RALEIGH NEW YORK LISBON SINGAPORE

BITSIGHT