



WEB APPLICATIONS
SECURITY STATISTICS REPORT
2016

INTRODUCTION

This year WhiteHat Security™ celebrates its fifteenth anniversary, and the eleventh year that we have produced the Web Applications Security Statistics Report. The stats shared in this report are based on the aggregation of all the scanning and remediation data obtained from applications that used the WhiteHat Sentinel™ service for application security testing in 2015. As an early pioneer in the Application Security Market, WhiteHat has a large and unique collection of data to work with.

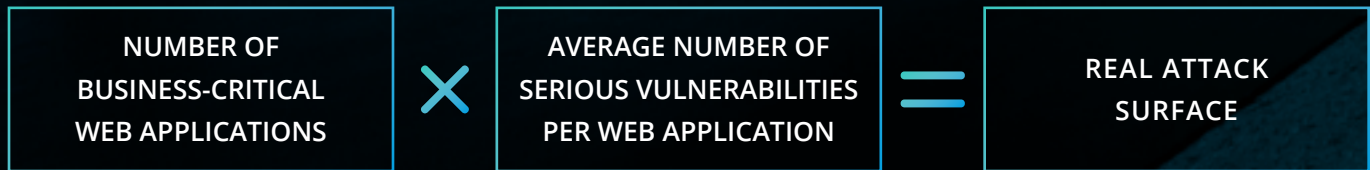
Rather than provide a lengthy analysis of the data in this Stats Report in this introduction, we've decided instead to provide some "what this means to you" commentary at the end of the three main sections of the report; commentary that attempts to make the data relevant to Executives, Security practitioners and DevOps professionals. Security is a concern that spans multiple teams in an organization – from the board and C-suite, to IT and development teams, to the security team and beyond – and the data in this report will mean different things to these different audiences.

A couple of parting thoughts before we dive into the 2015 stats:

"Web application attacks represent the greatest threat to an organization's security."

Web application attacks represent the greatest threat to an organization's security. Web app attacks represented 40% of breaches in 2015¹. This number is staggering, but not surprising, when you consider that, according to Gartner estimates², only \$591.5 million was spent on security testing products worldwide in 2015. This number is significantly lower than the spend on other types of security products. The line item on the security checklist that could have the biggest impact on an organization's security posture gets the least amount of attention or funding.

Although the data in this report helps to identify and scale the web application problem, it doesn't do justice to the real equation everyone involved in securing an organization should keep in mind:



Across industries, we have observed that organizations have hundreds, if not thousands, of consumer facing web applications, and each of those websites has anywhere from 5 to 32 vulnerabilities per web site. This means that there are thousands of vulnerabilities across your web applications.

This is the scenario that keeps the team at WhiteHat Security up at night. This equation is the problem we're trying to fix in order to put the odds in your favor, regardless of what kind of organization you are, or what industry you play in.

These vulnerabilities increase the total business risk that organizations assume and pass along to users of their vulnerable web applications. Understanding your company's overall web application security posture has to be simplified as the attack surface expands with the increasing number of business critical web applications and an increasing number of consumers of your web applications.

The graph below represents data from all WhiteHat Security customers with web applications under management by WhiteHat Sentinel. Keeping in mind that the higher the number, the better the security, we can see that less than 5% of the sites have an exceptional application security profile with a score of more than 700. About 40% of the applications have a score below 500, indicating they have a lot of room for improvement in application security.

WHITEHAT SECURITY INDEX DISTRIBUTION FOR ALL SITES

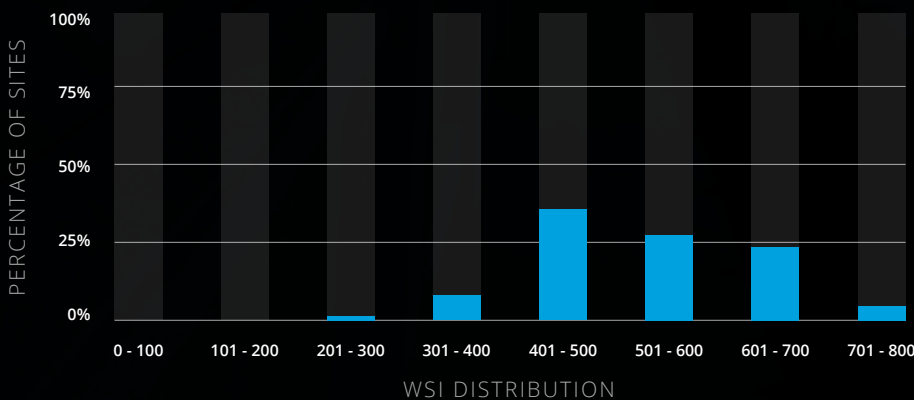


FIGURE 1:

WSI is a measure of a website's security profile, based on a multitude of data signals that impact the security status and change over time – information like website configuration, scanning frequency, vulnerability history, remediation rate, window of exposure and website complexity. The WSI is a single number, between zero and 800. The higher the number, the better the security.

This report starts by taking a look at the stats by industry, then takes a deeper dive into application security vulnerabilities, remediation and time-to-fix by vulnerability class and risk rating.

¹ Verizon 2016 Data Breach Investigations Report

² Gartner Inc., "Market Share: Security Software, Worldwide, 2015", Sid Deshpande, Ruggero Contu, 06 April 2016

TABLE OF CONTENTS



THE STATS BY INDUSTRY	5
APPLICATION SECURITY VULNERABILITIES	6
WINDOW OF EXPOSURE	7
AVERAGE VULNERABILITIES PER SITE	9
AVERAGE VULNERABILITY AGE BY INDUSTRY	11
REMEDIATING VULNERABILITIES	13
TIME-TO-FIX BY INDUSTRY	15
WHAT IT ALL MEANS	17



A DEEPER DIVE INTO VULNERABILITIES, REMEDICATION, AND TIME-TO-FIX	19
VULNERABILITY LIKELIHOOD BY CLASS	21
REMEDICATION BY CLASS	23
REMEDICATION BY CLASS: 2013 - 2015	25
AVERAGE TIME-TO-FIX	27
WHAT IT ALL MEANS	29



VULNERABILITY AGE, REMEDIATION RATE, AND TIME-TO-FIX BY RISK RATING	31
AVERAGE VULNERABILITY AGE BY RISK	33
REMEDICATION RATE BY RISK	35
AVERAGE TIME-TO-FIX BY RISK	37
WHAT IT ALL MEANS	39



CONCLUSION	41
ABOUT THIS REPORT	41
METHODOLOGY	42
ABOUT WHITEHAT SECURITY	42



THE STATS BY INDUSTRY



APPLICATION SECURITY VULNERABILITIES

Web application vulnerabilities continue to be a significant problem. Depending on the specific circumstances, these vulnerabilities could cause significant problems for the companies that have not remediated them, up to and including the theft of critical business data or personally identifiable information, web site defacement, or denial of service.

Most web sites are vulnerable most of the time. The average age of an open critical vulnerability is over 300 days; high-risk vulnerabilities have an average age of more than 500 days. (Note that vulnerability age is calculated only for open vulnerabilities. This means that if vulnerabilities tend to remain open, the average age will be high. If most vulnerabilities have been opened only recently, the average age will decrease.)

This section addresses the average number of vulnerabilities per web site that a business within a given industry can expect to have; the average age of vulnerabilities by industry; and remediation rates per industry. Following the charts is information on what these statistics mean to the various professionals within an organization who are responsible for managing cyber security and risk.



WINDOW OF EXPOSURE

Window of exposure is defined as the number of days an application has one or more serious vulnerabilities open during a given time period. Window of exposure is categorized as:

ALWAYS VULNERABLE:

A site falls in this category if it is vulnerable on every single day of the year.

FREQUENTLY VULNERABLE:

A site is called frequently vulnerable if it is vulnerable for 271-364 days a year.

REGULARLY VULNERABLE:

A regularly vulnerable site is vulnerable for 151-270 days a year.

OCCASIONALLY VULNERABLE:

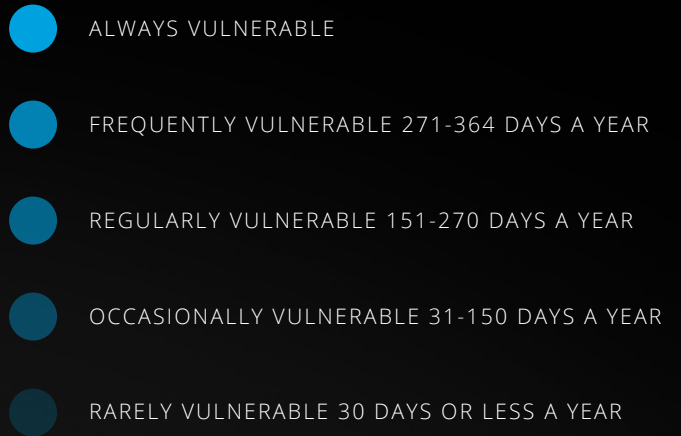
An occasionally vulnerable application is vulnerable for 31-150 days a year.

RARELY VULNERABLE:

A rarely vulnerable application is vulnerable for less than 30 days a year.

The graph shows that a substantial number of web applications remain always vulnerable. About one third of Insurance applications, about 40% of Banking & Financial Services applications, about half of Healthcare and Retail applications, and more than half of Manufacturing, Food & Beverage, and IT applications are always vulnerable. This implies that organizations are not able to resolve all of the serious vulnerabilities found in their applications, and it takes them a long time to remediate serious vulnerabilities.

FIGURE 2





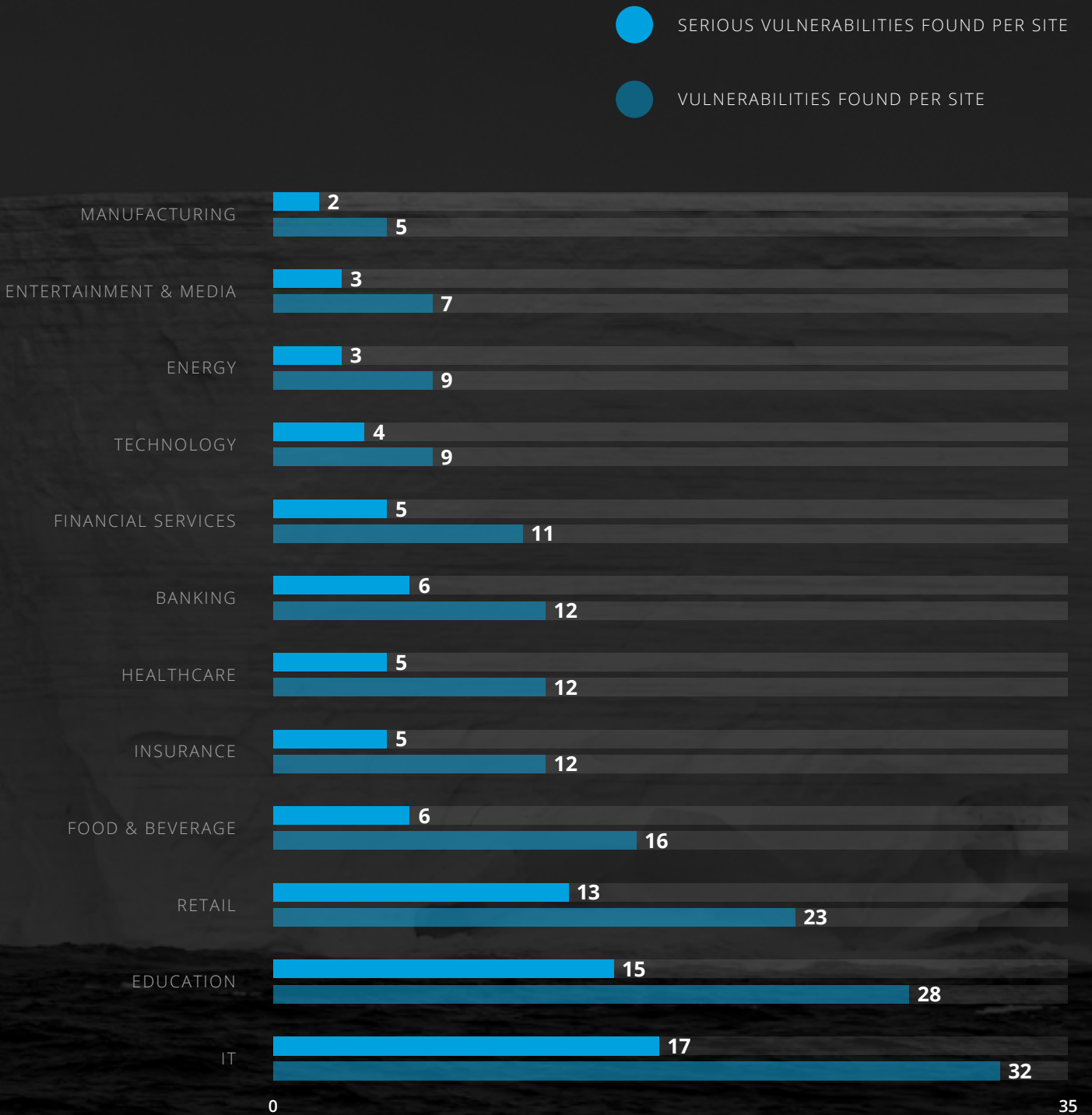
AVERAGE VULNERABILITIES PER SITE

Average vulnerabilities per site varies from five (in Manufacturing) to 32 (in IT). Regulated industries – such as financial services and healthcare – are not performing significantly better than the rest.

As the chart indicates, the Retail, Education and IT industries suffer the highest number of vulnerabilities – including serious vulnerabilities – of any other industry studied.



FIGURE 3





AVERAGE VULNERABILITY AGE BY INDUSTRY

Data shows that vulnerabilities stay open for a very long time. Critical and high-risk vulnerabilities have an average age of 300 and 500 days respectively.

The average age of vulnerabilities across different industries is similar. Information Technology (IT) is an exception with the *highest average age of 875 days*.

FIGURE 4





REMEDIATING VULNERABILITIES

Remediation rates are important to all security stakeholders. Some vulnerabilities are easier to remediate than others: generally speaking, the more critical or high-risk the vulnerability, the more complex they are to understand and fix.

Of the twelve types of industries represented in our data, only three (Manufacturing, Food & Beverage, and Entertainment & Media) have remediation rates over 50%. One possible factor contributing to their relatively high remediation rate may be that web applications in those industries tend to rely on very high brand equity; therefore, the risk of damage to the website resulting in damage to the brand is higher.

Technology, Energy, Retail, Financial Services, Education, Insurance, Banking, and Healthcare have remediation rates below 50%. Less than one fourth of known vulnerabilities are remediated in the IT industry.

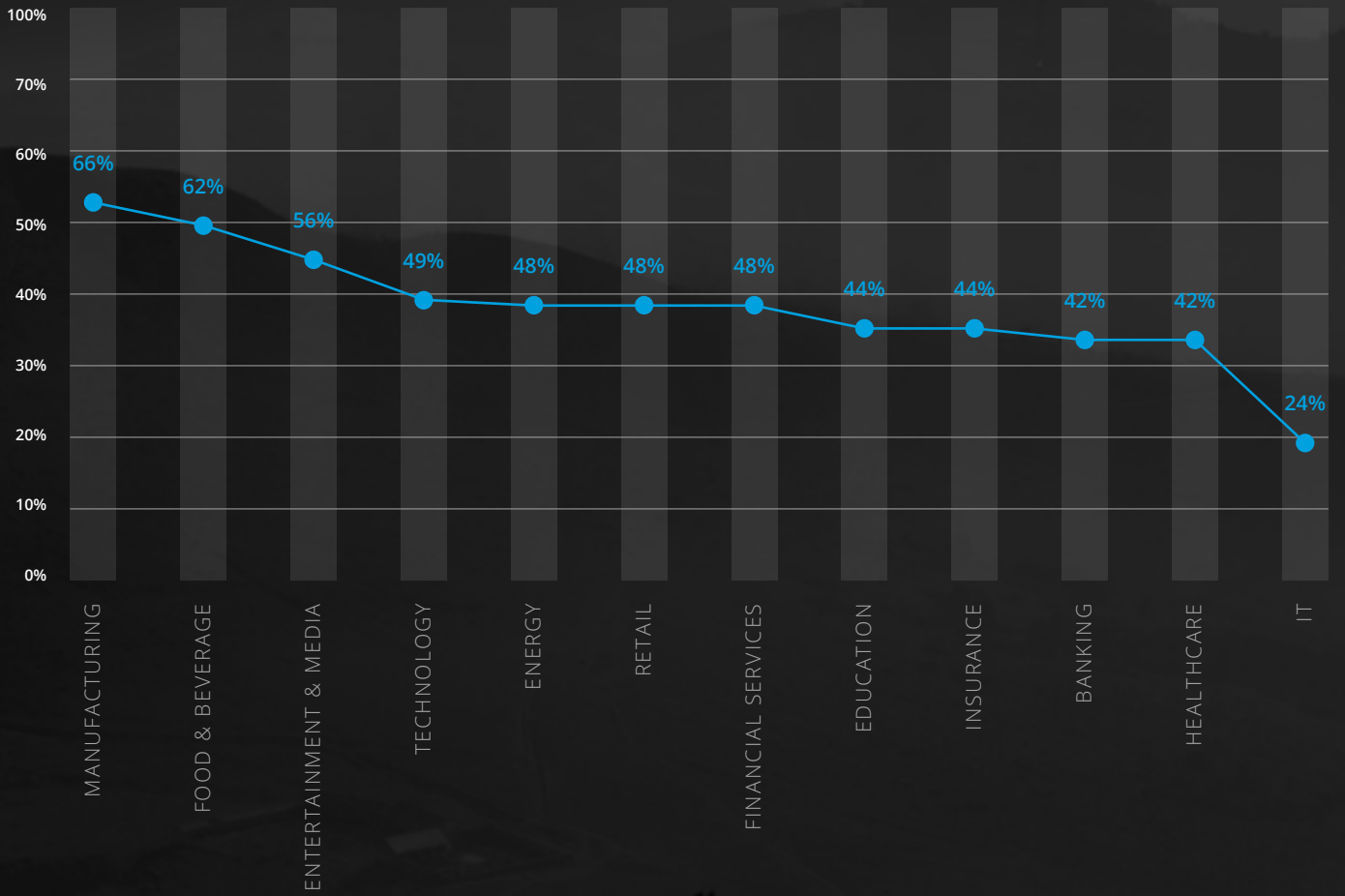
Remediation rates have improved in most industries. The greatest improvement was in the Food & Beverage industry, where remediation rates quadrupled (from 17% to 62%) over a two-year period. In Manufacturing, rates almost doubled (from 34% to 66%), and Healthcare and Insurance saw comfortable increases of over fifteen percentage points (26% to 42% for Healthcare and to 44% for Insurance), year over year. One explanation for these increases may be a greater investment in brand equity, which would lead to a greater concern for security.

Financial Services and Retail saw modest increases in their remediation rates over the last two years, from 41% to 48% for Financial Services and 42% to 48% for Retail industries.

Remediation rates have declined by ten points in Banking, from 52% to 42%, and significantly in IT, which saw a drop from a 46% remediation rate in 2013 to a 24% remediation rate in 2015.

FIGURE 5

REMEDIATION BY INDUSTRY





TIME-TO-FIX BY INDUSTRY

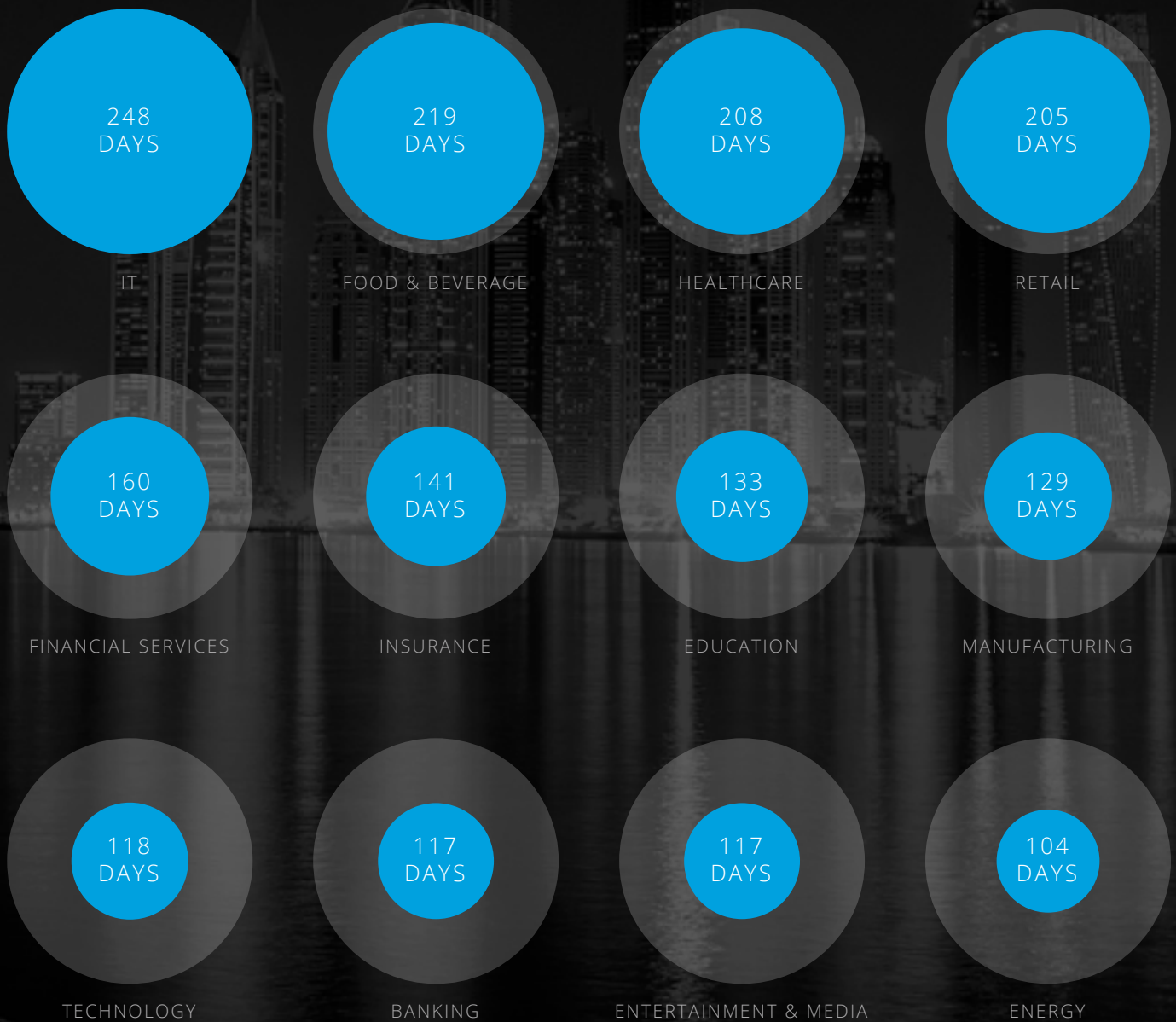
When vulnerabilities are found and security teams set out to fix them, how long does it take to implement the fix? The average time-to-fix varies by industry from approximately 100 days to 245 days.

The average time-to-fix vulnerabilities in the Retail and Healthcare sectors is around 200 days. Once again, IT is bringing up the rear when it comes to addressing vulnerabilities with average time-to-fix coming in at approximately 250 days.

Not only are the number of vulnerabilities found very high across industries including highly regulated industries, but also the remediation rates are uneven. Sectors like Retail and IT have a large number of serious vulnerabilities but the lowest remediation rates.

Highly regulated industries like Healthcare, Banking and Financial services have lower remediation rates when compared to other sectors.

FIGURE 6

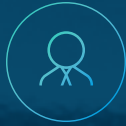




WHAT IT ALL MEANS

WHAT THIS MEANS TO

EXECUTIVES



FINDINGS

Regardless of your industry, it is likely that you have a large number of applications that are always at risk.

For example, when you look at Retail, over 50% of Retail sites are always vulnerable. The average number of vulnerabilities per site is 23, of which 13 are serious vulnerabilities. Of these 23 vulnerabilities, ~ 48% of these vulnerabilities will eventually get remediated and each of these vulnerabilities will take over 200 days to remediate.

Application security flaws are costly to fix as they require more than configuration changes. The cost of making a change is often perceived to outweigh the risk organizations are taking on. Our report shows that most vulnerabilities are serious, exposing your business to loss of data, revenue, reputation, and potentially customers.

Most businesses address their needs through more software, newer software and different kinds of software. Whether developed in-house, purchased, or outsourced, almost all software introduced into a business is done with speed and time-to-market in mind. Your IT team is introducing security flaws unknowingly as the software is built or integrated into your environment, and *your business is undertaking the risk because competition is catching up.*

RECOMMENDATION

We suggest that you build a scorecard for your industry and assess your current security posture based on our industry classification.

Get your arms around the security of your entire application landscape by using analytics to identify and prioritize the most business critical applications that need to be secured.

Inculcate a “mitigate immediately as you remediate” – or “block and fix” mindset. Mitigation is the first step, remediation is the final step to resolve security flaws in software.

Empower your security practitioners to hold development teams accountable for application security before your development team disengages from the project.

WHAT THIS MEANS TO

SECURITY PRACTITIONERS



FINDINGS

Based on the data we have presented, it is clear that most application security programs that security practitioners run are not 100% effective. Armed with data about industry wide remediation rates, security practitioners should be able to baseline their security posture and improve from there.

RECOMMENDATION

Security practitioners need to influence without authority. While they are the gatekeepers of security, they have little or no authority over the security quality of applications.

Security practitioners need to become a part of the continuous integration process that takes applications from code to production.

By using their knowledge of security and application security analytics throughout the development lifecycle, security practitioners can become development partners to produce secure quality code.

Security practitioners should lean on their vendors to give them the evidence and the tools they need to engage development teams in secure coding practices.

WHAT THIS MEANS TO

DEVOPS



FINDINGS

Actionable vulnerability data for staged applications is seldom available to developers in the development cycle. Our experience is that DAST scans are almost always performed at the periphery of the software release cycle.

Hence, application security flaws become known too late in the continuous integration process; oftentimes, the flaws become known only after the application has gone into production.


RECOMMENDATION

Assessing software for security close to production or release, and not earlier in the development process, is too late. Start assessing software for security closer to development.

Employ both source scanning and dynamic scanning as your organizations move to a continuous integration process.



**A DEEPER DIVE INTO VULNERABILITIES,
REMEDiation, AND TIME-TO-FIX**



In this section, we'll look at the various classes of vulnerabilities, and study their likelihood, remediation rate, and time to fix.



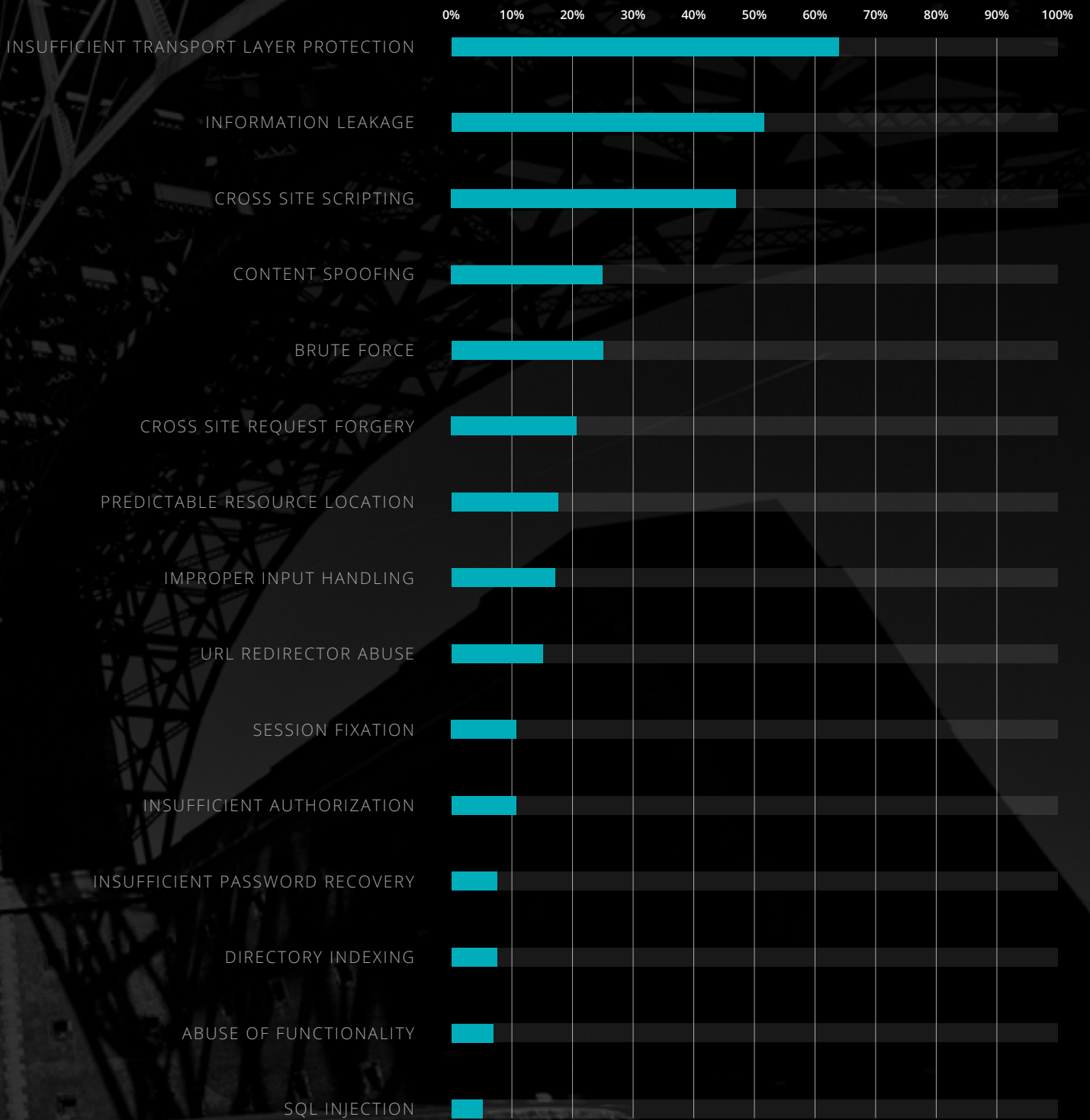
VULNERABILITY LIKELIHOOD BY CLASS

Vulnerabilities fall into different “classes”, or categories, that have unique attributes. For example, Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted web sites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it. [Source: https://www.owasp.org/index.php/Cross-site_Scripting_\(XSS\)](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS))

The Percent Likelihood seen in the graph reflects how likely it is that a site will have a *specific* class of vulnerability. This is calculated based on the number of sites that have at least one open vulnerability in a given class compared to the total number of active sites under WhiteHat Sentinel service.

To learn more about all of these vulnerabilities, visit http://projects.webappsec.org/f/WASC-TC-v2_0.pdf.

FIGURE 7





REMEDIATION BY CLASS

As you can see in the graph, remediation rates vary substantially by class.

Insufficient Transport Layer Protection vulnerabilities are relatively easy to fix by applying patches, so this class of vulnerability enjoys the highest remediation rate, at 61%. Conversely, **Brute Force** and **Insufficient Password Recovery** attacks have the lowest remediation rates, at 23% and 22% respectively. This is probably due to the complex inter-relationship between password recovery, brute force attacks, and denial of service. Brute Force attacks are frequently used to compromise passwords; the most reliable way to prevent them is to limit the number of attempts that can be made for a given username. However, this in turn can contribute to denial of service attacks, creating a vicious cycle of cause and effect. These complications may be responsible for the low remediation rates for these classes.

FIGURE 8



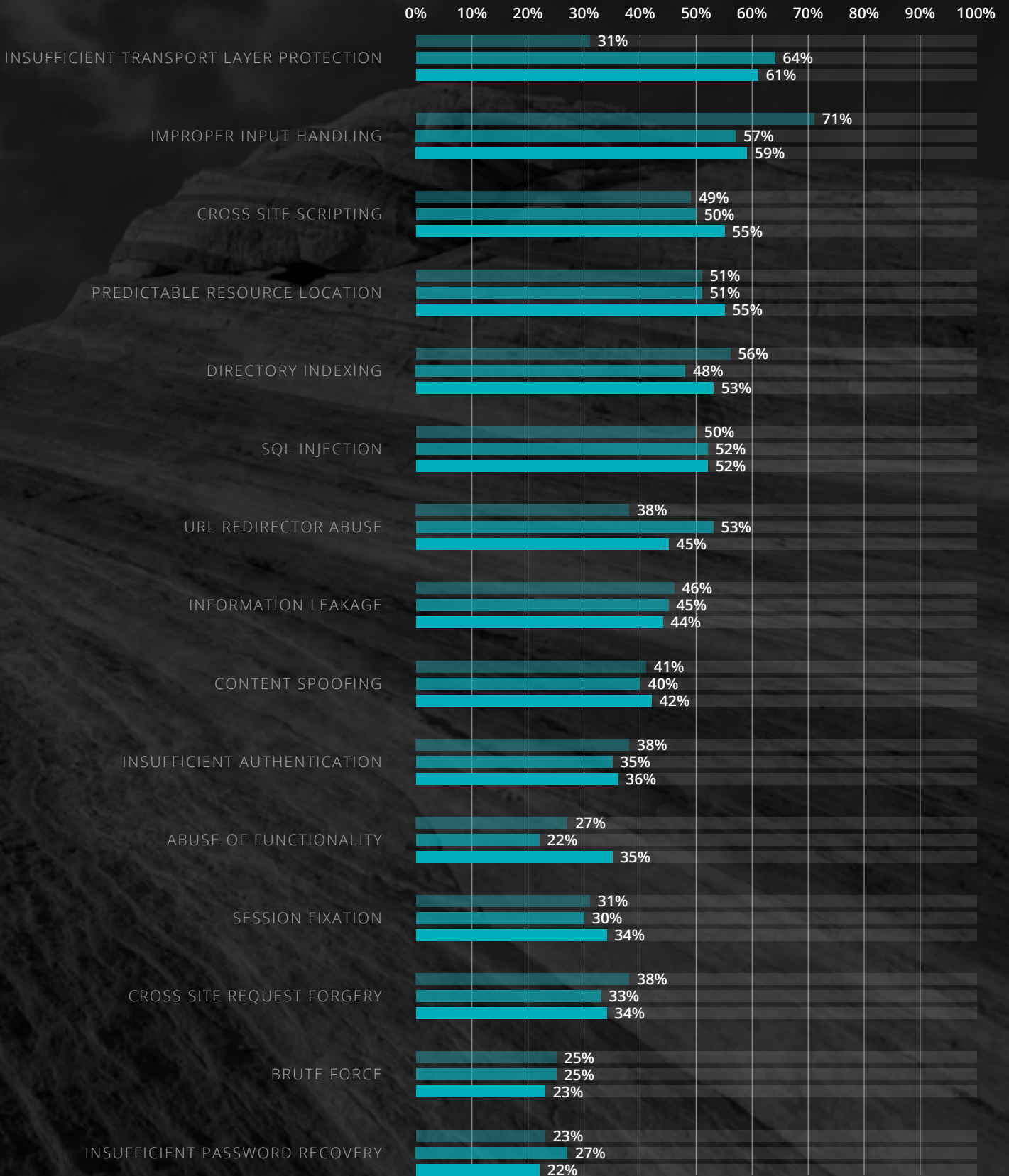


REMEDIATION BY CLASS: 2013 - 2015

Looking back over the last few years, remediation rates have been improving only very incrementally for the majority of the vulnerability classes.

FIGURE 9

2013 2014 2015





AVERAGE TIME-TO-FIX

On average, it takes approximately 150 days to fix vulnerabilities. Critical vulnerabilities are not resolved significantly more quickly than the rest, and high-risk vulnerabilities actually take the most time to fix. This may reflect a greater level of complexity, or that when organizations have the resources to fix only some vulnerabilities, the critical vulnerabilities will be resolved first and the remainder are resolved as resources are available – with simpler fixes being performed first, regardless of the risk level.

Unfortunately, after trending downwards in 2013, the average time to fix vulnerabilities has been steadily going up.



FIGURE 10 AVERAGE TIME-TO-FIX BY CLASS IN DAYS

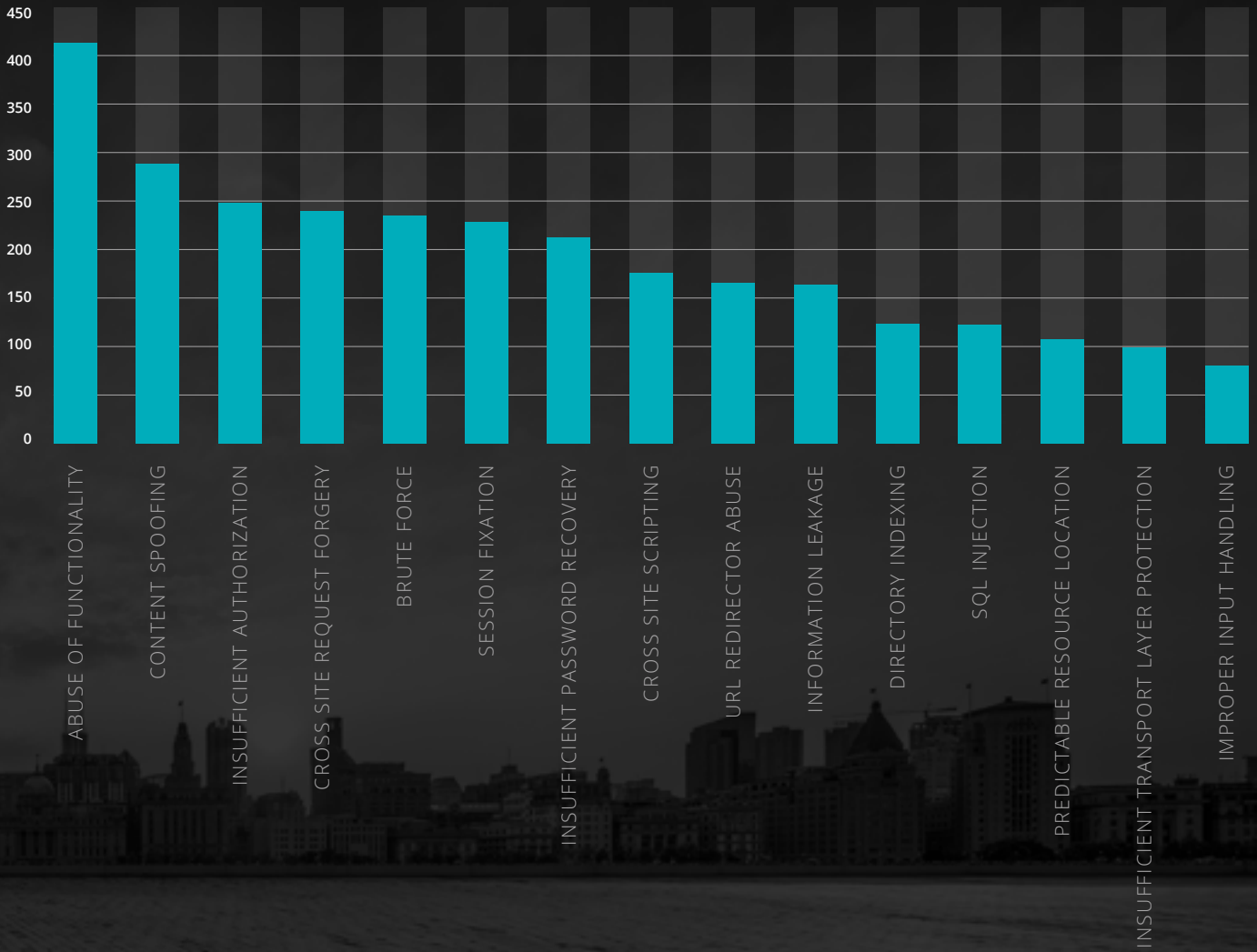
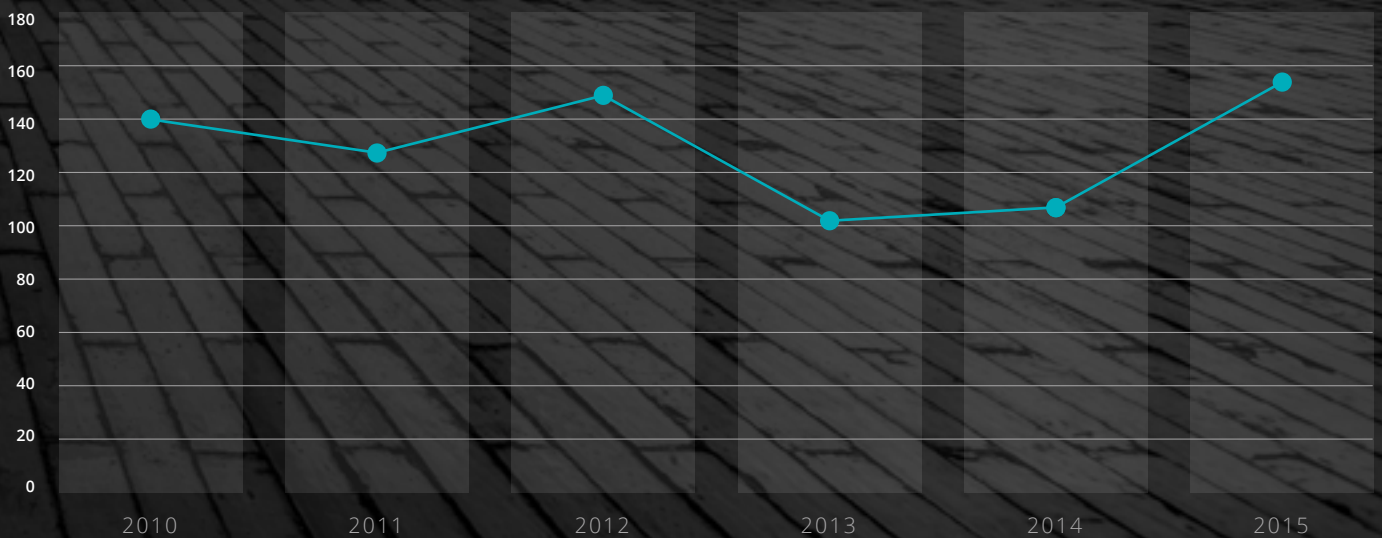


FIGURE 11 AVERAGE TIME-TO-FIX IN DAYS



A dark teal landscape with a sun or moon in the sky and a white border. The scene is a stylized, monochromatic landscape with a sun or moon in the sky and a white border. The text "WHAT IT ALL MEANS" is centered in the middle of the image.

WHAT IT ALL MEANS

WHAT THIS MEANS TO

EXECUTIVES



FINDINGS

Our data suggests that vulnerability likelihoods are very high and that the remediation rates are low. In addition, the remediation rates over the last couple of years have not improved dramatically.

The types of software vulnerabilities that plague organizations have more or less remained the same in recent years.

The longer a vulnerability remains open, the more exposed an organization is to threats. With most vulnerabilities remaining open for 150 days (five months), and critical or high-risk vulnerabilities often taking up to a year or more to fix, that's a long time for an organization in any industry to essentially keep the windows open for an attacker to get in.

RECOMMENDATION

Application security needs to become a board level conversation in your organization if it is not already. Executive sponsorship for application security should be outcome oriented to change the status quo.

Create an executive mandate to reward development teams for measuring and improving the security posture of their applications.

Make sure your security leaders have the resources they need to identify and fix vulnerabilities in software faster. The sooner they can remediate vulnerabilities, the less likely your organization will be to suffer the kind of debilitating breach that can come through your critical business applications.

Empower your security practitioners to create security programs that get visibility at the board level.

WHAT THIS MEANS TO

SECURITY PRACTITIONERS



FINDINGS

In the last three years, the likelihood of the top three software vulnerabilities has remained virtually the same. Based on this observation, it is likely that your security program is not driving remediation.

Driving your teams to prioritize and fix these vulnerabilities will produce positive business outcomes for your organization.

RECOMMENDATION

Identify security patches required for the underlying operating system to provide your business applications a secure execution environment. Work with IT to identify scheduled maintenance windows aimed at updating the OS for security patches.

Help your development teams understand the composition of their software applications and prioritize the vulnerable libraries for your development teams to fix/upgrade. Often developers are overwhelmed with the sheer volume of vulnerabilities that open source libraries present.

WHAT THIS MEANS TO

DEVOPS



FINDINGS

Using the analysis presented above, it is evident that many development organizations are not using secure coding practices. Based on the data we present, development teams can improve the overall software security by focusing on fixing a small number of the most likely vulnerabilities.

For example, security flaws like Cross Site Scripting can easily be fixed if discovered in time. Cross Site Scripting continues to be a critical software vulnerability.

RECOMMENDATION

Developer training, frequent software assessment and developer analytics are key to implementing a security program that integrates with your organization's software development lifecycle.

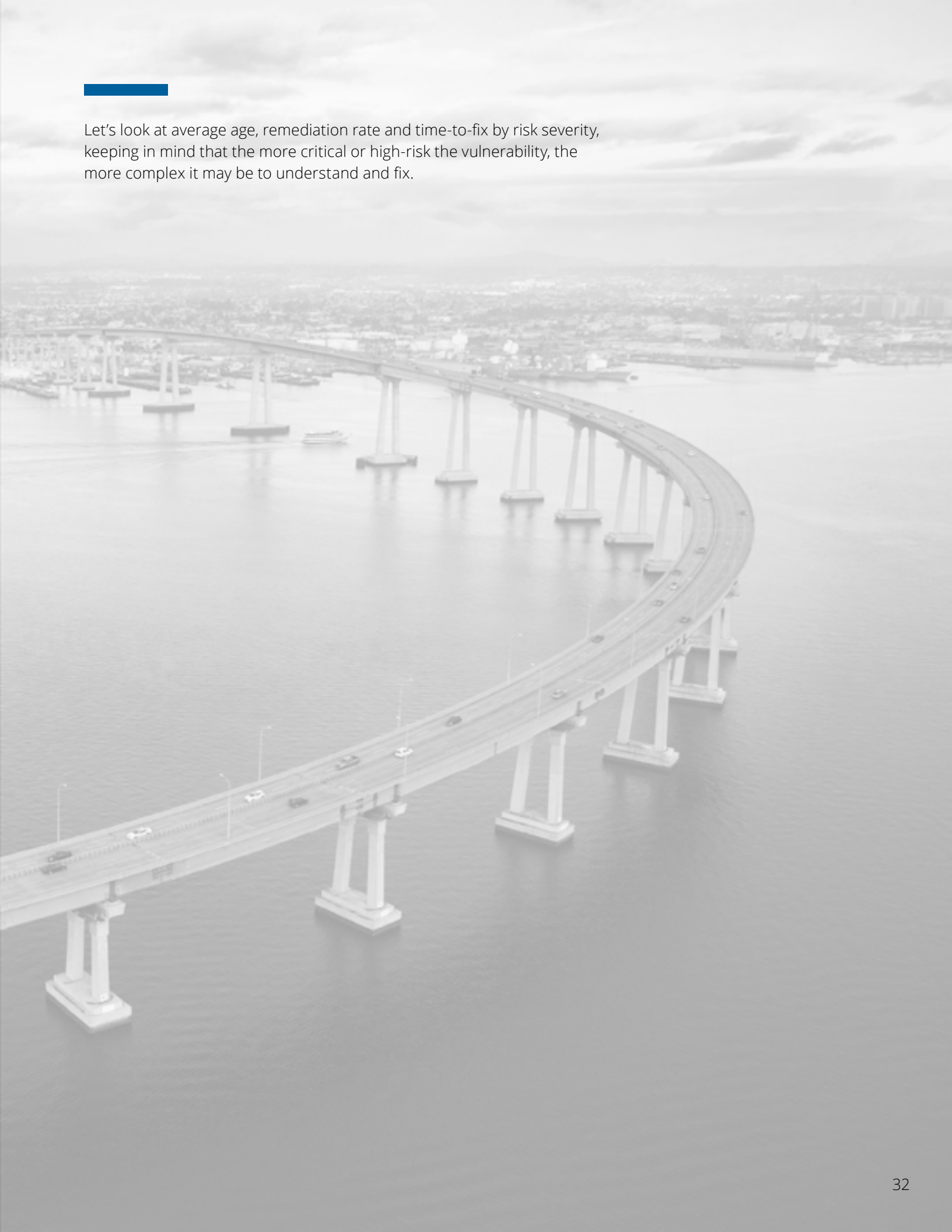
Create a culture that rewards writing security flaw-free code.

Use application security tools and experts to perform security quality checks on your code, much like you use software quality tools and experts.

An aerial photograph of a harbor filled with numerous sailboats. In the foreground, a multi-lane bridge spans across the water. The background shows a cityscape with various buildings and structures. The entire image is overlaid with a dark, semi-transparent filter, and a bright blue border frames the content.

**VULNERABILITY AGE, REMEDIATION RATE,
AND TIME-TO-FIX BY RISK RATING**

Let's look at average age, remediation rate and time-to-fix by risk severity, keeping in mind that the more critical or high-risk the vulnerability, the more complex it may be to understand and fix.

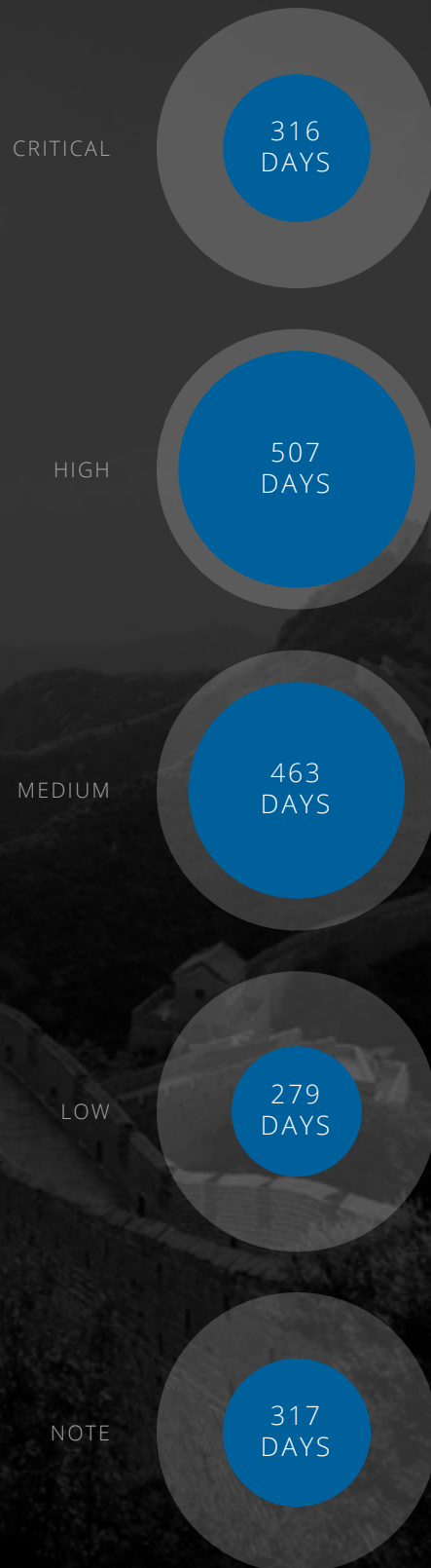


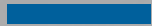


AVERAGE VULNERABILITY AGE BY RISK

Interestingly, vulnerabilities rated as a critical risk have approximately the same average age as “note” vulnerabilities, which are primarily minor deviations from best-practice or industry standards. Low-risk vulnerabilities actually have a lower average age than critical risk vulnerabilities, and a substantially lower average age than high- or medium-risk vulnerabilities; this may be due to a combination of the difficulty of remediating critical or high-risk vulnerabilities and a lack of security expertise.

FIGURE 12





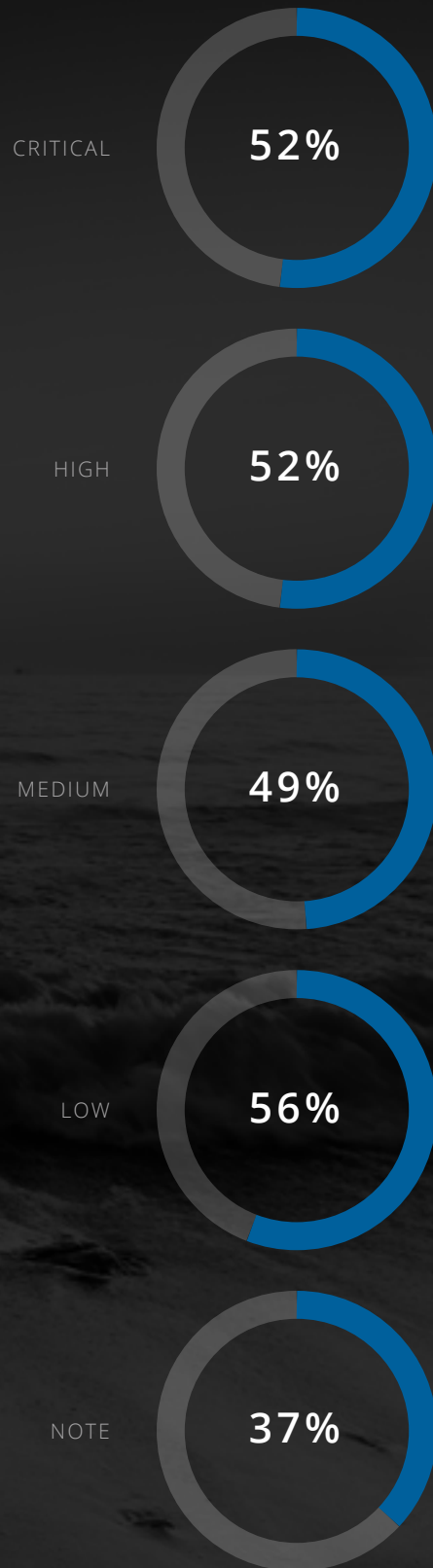
REMEDIATION RATE BY RISK

Remediation rates for critical, high, medium and low rated vulnerabilities are about the same.

Vulnerability ratings depend on many factors (e.g., business criticality of the asset, nature and amount of data stored, type of vulnerability, etc.). A vulnerability that is considered critical by one organization may be considered high or medium by another organization. As a result, remediation rates across rating levels from low to critical are not remarkably different.



FIGURE 13





AVERAGE TIME-TO-FIX BY RISK

In the previous section, we looked at average time-to-fix by vulnerability class. Here, we look at the average time-to-fix by the five risk ratings.

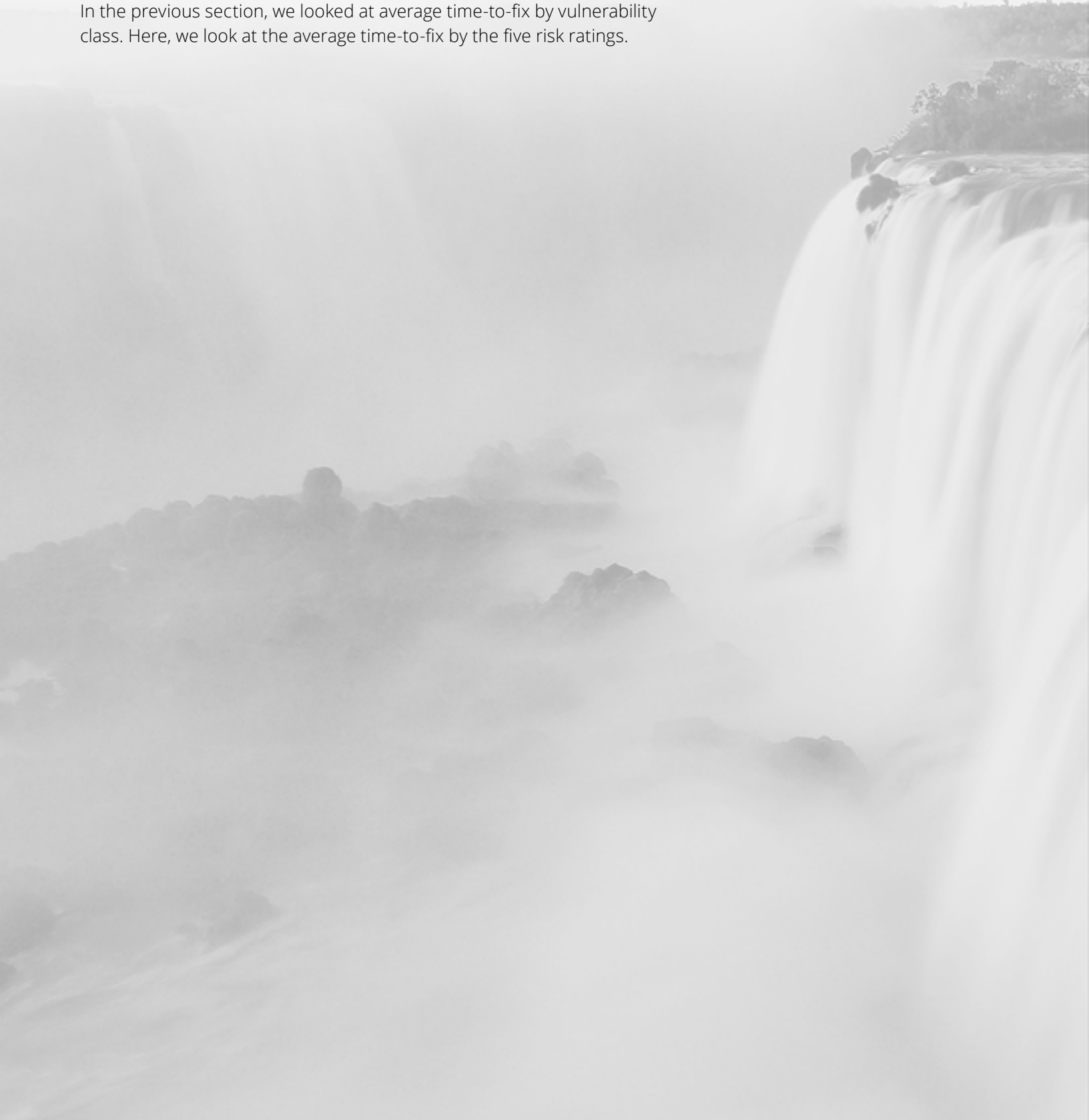



FIGURE 14





WHAT IT ALL MEANS

WHAT THIS MEANS TO

EXECUTIVES



FINDINGS

Based on our data, the expected correlation between the criticality of vulnerabilities found and the number of vulnerabilities remediated is absent. This finding suggests that systematic risk-based prioritization of security vulnerabilities is not being performed.

Software seldom makes it to production when there are critical software quality flaws, so why does software with critical security flaws make it to production?

Security flaws are not seen as quality flaws. Security is a non-functional requirement – but one that has the potential to damage the reputation of the organization. To enforce a systematic remediation strategy for security vulnerabilities, application security has to become a board level initiative.

RECOMMENDATION

Security is now a boardroom discussion topic; if it isn't yet in your organization, you should make it one. As the executive responsible for security, leverage application security analytics to not only measure your security posture but also to quantify risk to the business based on application security analytics – for example, compare your organization's security posture with your peers.

Often, security goals manifest themselves as a measure of adherence to corporate security policies. Simplify the security goals to be measured on a scale like one's "FICO®" score. This score should take into account the security of the software – such as the number of vulnerabilities found, how many of the vulnerabilities your team mitigates, and the time it takes them to remediate vulnerabilities. A FICO score like this can be used to indicate the level of risk and hence, an approximation on the probability you will be hacked.

WHAT THIS MEANS TO

SECURITY PRACTITIONERS



FINDINGS

Critical and high-risk vulnerabilities have an average age of 300 and 500 days respectively.

When this trend is compared with the trend to fix software quality flaws, it is quite evident that the SLA for fixing critical and high-risk security vulnerabilities is often not set or enforced.

Continuous security assessments and remediation should become an integral aspect of good software delivery.

RECOMMENDATION

Security practitioners should participate in development meetings to drive the secure application agenda.

By prioritizing the critical and high-risk security flaws for remediation, security professionals can help reduce the number of days serious vulnerabilities remain open.

Security professionals should immediately create a plan to mitigate critical vulnerabilities by using technologies like web application firewalls (WAFs) to provide development teams the necessary time to produce the remediation fix.

Security practitioners should plan static application testing cycles throughout the software development lifecycle and baseline the security characteristics of the software. By performing and reviewing the results against dynamic application security testing on staged applications, security practitioners can help development teams correlate security flaws manifesting in runtime with vulnerable software code. This reduces the number of critical and high-risk vulnerabilities that go out in the first place.

WHAT THIS MEANS TO

DEVOPS



FINDINGS

The trend of serious vulnerabilities open for >300 days does not align with DevOps principles. DevOps is all about reducing time-to-market and increasing the feedback loop.

It is likely that serious vulnerabilities are not being prioritized in subsequent sprints. The fact that development professionals with security experience are difficult to find further aggravates the situation.

RECOMMENDATION

The product teams responsible for continuous delivery and DevOps need to be trained on security principles, best practices and writing secure code to address the top security vulnerabilities manifesting in production code. This will enable you to hold the product teams and developers accountable for application security.

DevOps teams are driven by user stories which have constraints and acceptance criteria. Along with functional and performance-based constraints and acceptance criteria, the user stories should also incorporate application security as a part of the constraints and acceptance criteria.



CONCLUSION

Organizations must cultivate a culture of cross-team collaboration and cooperation to prioritize application security.

Application security solutions have been around for years, yet vulnerabilities remain rampant, and it still takes too long to get them fixed. The primary take-aways for the key stakeholders are:

- Executives need to fully understand the risks to the business and engage with all of the teams involved in protecting the business.
- Security leadership and front-line practitioners must advocate for making the right investments in both technology and people to secure the business.
- Developers and IT teams need to make security as much of a priority as functionality when developing, customizing or implementing applications.

Easier said than done, but necessary to adequately protect the business, its customers, and its ecosystem.

ABOUT THIS REPORT

The WhiteHat Security Web Applications Security Statistics Report provides a one-of-a-kind perspective on the state of web application security and the issues that organizations must address in order to conduct business online safely.

Web application security is an ever-moving target. New websites launch, new code is released, and new web technologies are rolled out every day; and every day, new attack techniques are being developed that put every online business at risk. Businesses must have timely information about how to defend their websites, evaluate the performance of their security programs, and understand how their vulnerability levels compare with their industry peers. Without this information, businesses cannot stay ahead of attackers and continue to maintain – much less improve — enterprise website security.

To provide this information, WhiteHat Security has been publishing its Web Applications Security Statistics Report since 2006. This report focuses exclusively on vulnerabilities in custom web applications. The underlying data comprises vulnerability assessment results from tens of thousands of websites across hundreds of well-known organizations, and represents the largest and most accurate picture of web application security currently available. From this data we can identify prevalent vulnerabilities, remediation rates, time to fix, and how businesses can measurably improve any application security program.



METHODOLOGY

This analysis is based on the aggregation of all the scanning and remediation data obtained from applications that use the WhiteHat Sentinel service for security testing. Data is segmented along multiple dimensions, including risk levels, vulnerability classes, and industry.

- Risk levels are based on the OWASP rating methodology. Vulnerabilities are rated as Critical, High, Medium, Low, and Note. (critical and high-risk vulns taken together are referred to as “serious” vulnerabilities.)
- Vulnerability classes are based on WASC threat classification.
- Industry information for sites is provided by customers.

We have analyzed this data using key indicators that include the likelihood of a given vulnerability class, remediation rates, time to fix, and age of open vulnerabilities. (These are among the key indicators used to calculate the WhiteHat Security Index for assets covered by Sentinel.) However, some biases may be intrinsic to the data source -- for instance, a site that was recently on-boarded to Sentinel will have a much lower Open Vulnerability Age for any of its vulnerabilities than a site that has been using Sentinel longer. Different service levels for different sites also mean that some vulnerabilities may be more likely to be discovered than others. Finally, tests are continually evolving, and change in tests over time may affect apparent trends.

About WhiteHat Security

WhiteHat Security has been in the business of securing web applications for 15 years. Combining advanced technology with the expertise of its global [Threat Research Center](#) (TRC) team, WhiteHat delivers application security solutions that reduce risk, reduce cost and accelerate the deployment of secure applications and web sites. The company’s flagship product, [WhiteHat Sentinel](#), is a software-as-a-service platform providing dynamic application security testing (DAST), static application security testing (SAST), and mobile application security assessments. The company is headquartered in Santa Clara, Calif., with regional offices across the U.S. and Europe. For more information on WhiteHat Security, please visit www.whitehatsec.com, and follow us on [Twitter](#), [LinkedIn](#) and [Facebook](#).

WEB APPLICATIONS SECURITY STATISTICS REPORT 2016

WHITEHAT SECURITY, INC.

3970 Freedom Circle Santa Clara, CA 95054 • 1.408.343.8300 • www.whitehatsec.com
© 2016 WhiteHat Security, Inc. All rights reserved. WhiteHat Security™, WhiteHat Sentinel™ and the WhiteHat Security™ logo are trademarks of WhiteHat Security, Inc. All other trademarks or service marks are the property of their respective owners.

