Brought to you by:

CYCOGNITO

External Exposure & Attack Surface Management

for dummies®
A Wiley Brand

Find assets attackers could use against you

Map your organization's exposed risks

Prioritize and remediate what really matters

CyCognito
Special Edition

Steve Kaelble
Rob Gurzeev
Dima Potekhin

About CyCognito

We are CyCognito, a new approach to external risk exposure management driven to create positive business impact. Our platform helps organizations identify, understand, and master their external security risk.

Fully automated, highly scalable, and designed to function as promised, our platform uses advanced machine learning and natural language processing to allow for unprecedented reach, speed, and accuracy. We can step into the shoes of potential attackers — which in turn helps us identify and secure gaps better than anyone. We help teams secure their external attack surface by helping them determine true risk exposures, where they need to focus, and how they should invest. And then we use what we learn to help bridge cyber risk remediation across departments unlike ever before.

Our platform is oriented around four intertwined primary capabilities that accelerate risk remediation: Discovery, Contextualization, Security Testing, and Prioritization. Together, these capabilities form the backbone of our platform helping you eliminate external risk exposures.

External Exposure & Attack Surface Management

CyCognito Special Edition

by Steve Kaelble, Rob Gurzeev, and Dima Potekhin

for dummies®
A Wiley Brand

External Exposure & Attack Surface Management For Dummies®, CyCognito Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: WHILE THE PUBLISHER AND AUTHORS HAVE USED THEIR BEST EFFORTS IN PREPARING THIS WORK, THEY MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES REPRESENTATIVES, WRITTEN SALES MATERIALS OR PROMOTIONAL STATEMENTS FOR THIS WORK. THE FACT THAT AN ORGANIZATION, WEBSITE, OR PRODUCT IS REFERRED TO IN THIS WORK AS A CITATION AND/OR POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE PUBLISHER AND AUTHORS ENDORSE THE INFORMATION OR SERVICES THE ORGANIZATION, WEBSITE, OR PRODUCT MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING PROFESSIONAL SERVICES. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR YOUR SITUATION. YOU SHOULD CONSULT WITH A SPECIALIST WHERE APPROPRIATE. FURTHER, READERS SHOULD BE AWARE THAT WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ. NEITHER THE PUBLISHER NOR AUTHORS SHALL BE LIABLE FOR ANY LOSS OF PROFIT OR ANY OTHER COMMERCIAL DAMAGES, INCLUDING BUT NOT LIMITED TO SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGES.

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

ISBN 978-1-394-15385-5 (pbk); 978-1-394-15386-2 (ebk)

Publisher’s Acknowledgments

We’re proud of this book and of the people who worked on it. Some of the people who helped bring this book to market include the following:

Project Manager: Rebecca Senninger

Acquisitions Editor: Traci Martin

Senior Managing Editor: Rev Mengle

Client Account Manager: Matt Cox

Production Editor: Saikarthick Kumarasamy

CyCognito Contributers: Gregory Delaney, Jason Pappalexis, Emma Zaballos, Carrie Oakes

Table of Contents

Introduction

Your enterprise has far more digital assets in its inventory than ever before, including web apps, cloud-based storage, Internet of Things (IoT) devices, application programming interfaces (APIs), and a whole lot more. Now, multiply that across your information technology (IT) ecosystem. The result? Your external attack surface is populated by countless Internet-facing assets — including some you aren't aware of. What's more, your risk accumulates when you're not keeping a close eye on these assets.

External exposure and attack surface management helps organizations to proactively know and manage their attack surface, reducing critical risks to the business. It's crucial to do this with an "outside in" perspective, that is to say, the viewpoint of an attacker. That's because today's attackers have perfected the art of discovering vulnerabilities and paths of least resistance that will lead them into your systems and to your vital digital assets. You have to get better and faster at finding and fixing all the paths and vulnerabilities, particularly the unknown ones.

An exposure management program starts with external attack surface management (EASM) to understand your assets and their responsible organization. However, mature exposure management goes beyond that. It continuously tests assets, assesses risks, and adapts to changes. It helps prioritize exposed risks and promptly addresses them before attackers strike. This work must scale to cover your entire attack surface without constant human effort.

About the Book

External Exposure & Attack Surface Management For Dummies, CyCognito Special Edition is your guide to solving this critical need. It's brought to you by experts who developed these crucial skills in the intelligence community and then launched a private enterprise to automate the process.

Read on and learn more about why this work is both challenging and essential. The book discusses the need to think like an attacker, the importance of having a full and carefully categorized inventory of all externally exposed digital assets up and down the ecosystem, and how you can uncover risk exposures that attackers can exploit.

Foolish Assumptions

In writing this book, we're making a few assumptions. You may be an IT security professional or engineer, or perhaps a leader on the business side. You know about the ever-growing threat to your digital assets, but fear it will be overwhelming to deal with all the issues you're sure to find. You also would appreciate insights into how to approach and consider the challenge of building an external exposure management program.

Icons Used in This Book

Check the margins of the book and you'll spot some icons. They're there to catch your eye and give you some guidance.

REMEMBER

This isn't a lengthy book, but if you're short on time, don't miss the point in the paragraph marked by this icon.

TIP

Our aim is to offer actionable information, and the paragraph marked by this icon has some helpful hints.

WARNING

Okay, you already know how dangerous it is out there, but this icon alerts you to a warning you should not ignore.

Beyond the Book

After reading this book, you'll know a lot about external exposure and attack surface management. Visit CyCognito's website for more insights and guidance.

IN THIS CHAPTER

- **Watching external exposures proliferate**
- **Seeing the challenges of today's environment**
- **Learning from the horror stories**
- **Enhancing your external exposure management**
- **Checking out the use cases**

Chapter 1
Moving Ahead Amid the Security Challenges

If you didn't relish change, you wouldn't have a career in cybersecurity or information technology (IT). But these days the changes in IT environments are downright dizzying and full of both opportunity and risk.

This chapter explores how those changes are inevitable and sometimes dangerous. It outlines why external attack surfaces are increasingly large and hard to manage. It shares a few scary headlines to make it clear what can go wrong. It introduces ideas for moving forward safely with confidence, and explores use cases for these concepts.

Keeping Up with External Exposure

The world has changed dramatically in recent years, and so have the IT environments that enable our work and many other elements of our lives. Developments have been downright breathtaking.

Virtually everything is more accessible, from information to entertainment to every service imaginable. Remote work has gone from nearly impossible, to a hassle, to pretty successful, to an essential way of life for many. Companies have moved on-premises apps and services to cloud-based environments to enable this accessibility, achieve flexibility and scalability, and implement new functionality quickly. It also, of course, helps them get a handle on capital expenses and other costs.

Software-as-a-Service (SaaS) and other subscription concepts have moved from being an interesting idea to a vital part of companies' IT infrastructure. They enable quick and easy implementations that help companies keep up with the competition while keeping costs in line.

There's much to like about this fast-changing world. New capabilities are unleashed faster and new customers are being reached where they are. The potential for business growth is tantalizing, so executives are happy. Rolling out new services through SaaS options is so easy that in some cases it requires little involvement or oversight by the IT department, which makes a lot of people happy. Customers like all the options and conveniences, so they're happy, too.

WARNING

You know who else is? Would-be cybercriminals. All this revolutionary change has greatly expanded attack surfaces, so bad actors are like unscrupulous kids in a candy shop with lots of tasty options available for shoplifting.

Who's *not* happy about all this? The people in charge of IT security. They have to keep all that candy out of the wrong hands — and there are a lot more hands to watch and candy to protect, stored in a lot more candy jars. Whoever's in charge of risk management may be grumpy, too, after enduring too many sleepless nights.

Creating New Challenges

It's pretty easy to use a credit card. Heck, these days you don't even have to swipe it — you just hold it near the card reader and watch four LEDs turn green. Who hasn't on occasion taken advantage of that transactional ease and later regretted it? Maybe you bought something a bit foolish on a whim or perhaps you forgot to tell your significant other about a purchase.

REMEMBER

Similar scenarios play out in the world of IT, particularly development in the cloud. They can be enabled quickly, even with a credit card, without fully considering the implications. This sometimes leads to shadow IT, where some type of software or other IT resource ends up being run as an extension of your organization's environment. And it's increasingly easy to forget to tell IT about it.

SaaS vendors can add to the shadow IT problem, too, such as when a startup provides a SaaS-based service for a financial institution. As vendors add tentacles to your IT environment, you can't always be certain that they're following the security standards you need.

"What's the big deal?" someone replies. After all, cloud environments are safe, aren't they? If they're properly configured, perhaps, but how can you ensure that's happening if cloud environments are implemented with such speed and lack of oversight? Do you really trust them to contain your proprietary business information? You may — and you may not.

WARNING

Adding to the challenges, some will attempt a lift-and-shift approach to move existing assets or infrastructure to the cloud. Doing that properly requires expertise that most organizations don't routinely have, and doing that improperly creates risk.

Put it all together and you can end up with a host of challenges and potential risks. For example, your organization might have exposed web apps with application programming interfaces (APIs) living out there in the increasingly fragmented IT environment.

You have more and more silos, too, which is usually not a good thing. There may be subsidiaries running in their own silos, and merger activity might bring in new siblings with differing security standards. And by the way, bad actors are well aware of how these risks present them with opportunities.

Learning Hard Lessons

The headlines are full of examples of what can go wrong when a person with malevolent intent finds a hole in the external attack surface. It's more challenging than ever to manage external exposures but also more important than ever. Here are just a few horrors of past catastrophes. Today's newspaper no doubt has a new one.

- **Western Digital:** In the spring of 2023, hackers claimed to have stolen some 10 terabytes of data from Western Digital, including vast stores of customer information. The hackers claimed to have gotten to this prize by exploiting an externally exposed vulnerability on the company's infrastructure, then traversing through in search of valuable information. The attackers said they were seeking a ransom totaling at least eight figures.
- **GoDaddy:** It's one of the world's biggest Internet domain registrars, and in early 2023 it announced there had been a security compromise over multiple years. Unknown attackers had been able to steal company source code, along with login credentials for customers and employees. The bad guys also were able to install malware redirecting customer websites. The company was prudently using a zero trust model but did not apply it across all login mechanisms — and any broadly accessible login page is an exposed risk. Attackers logged into a WordPress site with stolen credentials and were able to access a private key. And once someone has a private key, it's possible they can use it to access other areas or to impersonate the brand.
- **U.S. Department of Defense:** A trove of classified military information surfaced on social media in early 2023, covering the war in Ukraine and other highly sensitive topics. Turns out there was a misconfigured web server that didn't require a password, creating an exposed risk of the kind that adversaries often scan for. That was the biggest headline-getter in quite some time, but the reality is, the Defense Department data breaches are not so uncommon. A report in 2022 found that data breaches have more than doubled since 2015.

Building an External Exposure Management Program

In the good old days of not too long ago, you could think in terms of having a perimeter to defend. Due to the advent of the cloud, there really isn't a perimeter anymore, per se, or it's as vast as the sky itself. Your organization's IT environment has a huge amount of potential external exposure.

REMEMBER

We're pleased to offer a spoiler to that horror story, though: The cause is not hopeless at all. What you need to sleep better is a solid *external exposure management* program. That's what the rest of the book is about, but we'll give a basic overview here.

Notice that we said exposure management "program." It's a tool, but also more than that — it's a mindset and a way of operating to ensure your environment is as safe as it can be. It's really knowing your ecosystem of assets, examining for exposed risks, prioritizing your work based on the value of what those risks expose, and automating the work for continuous cadence and scale.

TIP

A key part of exposure management is the concept known as *external attack surface management* (EASM). You'll need a deep understanding and precise EASM approach and the technology to help your organization understand your Internet-exposed assets and what's at risk.

Exposure management goes a step further and helps you gain deep risk visibility so that you can see the vulnerabilities your attackers will be looking for. The aim, of course, is to see those vulnerabilities before they do and do something about them before they can be exploited. Exposure management adds to that visibility with active security testing at full scale, and helps you prioritize your remediation, then mobilize the response.

Through your exposure management program, you'll scan and test your external attack surface and figure out which risks need priority attention now, which can live further down the list, and which aren't really a concern. Then, you'll remediate and validate. You can sum it all up in terms of five key principles:

- **Know what you have:** You can't manage your assets until you know where they are and understand what they do.

- **Scan and test regularly:** Environments change all the time, introducing new risk exposures you need to know about.
- **Think like an attacker:** You'll be most successful if you put yourselves in the mindset of your adversaries and look at your exposures the way they would.
- **Be armed with evidence:** You have to be able to validate your findings and steer clear of false positives. This also helps to build trust cross-functionally and with third parties.
- **Have a solid process:** Establish how to handle what you find and how you will prioritize your findings so that you get the job done even when resources are limited.

Checking the Use Cases

REMEMBER

How does exposure management help your organization operate safely and securely in the IT environment of today and tomorrow? There are a number of key use cases for exposure management and external attack surface management:

- **Understanding all your brands:** This refers to how you identify and catalog all of the IT assets across the organization's infrastructure. Assets could include software applications, devices, network components, and other digital assets.
- **Asset inventory hygiene:** Once they're discovered, you need to create an up-to-date, complete inventory of assets. The inventory should track attributes such as ownership, location, configuration details, and running software.
- **Vulnerability risk management:** This refers to the process of identifying vulnerabilities, assessing them, prioritizing them, and then mitigating them. This involves regular vulnerability scanning, penetration testing, and prompt remediation.
- **Cloud visibility:** You'll never be able to manage exposures without understanding your cloud footprint, identifying any misconfigurations or questionable practices, and monitoring for exposures and access.

- **Due diligence for mergers and acquisitions:** You're making an acquisition to obtain something valuable to your organization, but you can also acquire vulnerabilities pretty easily. Exposure management and EASM help you evaluate the IT assets, vulnerabilities, and risks of the target company before they become your problems.
- **Scaling pen testers and red teamers:** You're doing penetration testing on the important stuff and wish you could do it on more, but hiring an army of pen testers is expensive and time consuming. Did you know pen testing involves a bunch of upfront tasks before any real-life hacking begins? Scoping the business, collecting open-source intelligence (OSINT), scanning IP-ranges, and identifying CVEs are necessary and time-consuming steps to plan their attack. Exposure and attack surface management can automate this upfront work. Then the real pen testing begins, exposing weaknesses that need to be fixed. They can do a lot more sophisticated work having saved all this time upfront.
- **Supply chain risk management:** Effective supply chains are increasingly interconnected, which adds value and streamlines business. However, the connections also open the door to new risks. You must assess and mitigate risks associated with vendors and suppliers at the same level as you would your own organization.

IN THIS CHAPTER

- Keeping an eye on the real problem of risk
- Viewing your organization the way an attacker would
- Benefiting from cyber expertise

Chapter 2 Thinking Like an Attacker

It's easy to think of external exposure management as a checklist that you must maintain, kind of like compliance. But if you're not keeping your eye on the specific assets that are actually at risk, you may be missing the point.

This chapter tells you why you must put yourself in the shoes of your adversary and look at your attack surface the way the they do.

Putting the Focus on Risk

REMEMBER

Managing your external exposures seems at first glance like an IT and compliance exercise, and it most certainly is. But it's much more — it's about understanding and mitigating risk. To gain the most solid protection from becoming a bad headline, your organization must adopt a risk orientation.

Compliance is focused on specific regulatory requirements but may miss many risks. Adopting a risk-focused approach lets you proactively identify and manage a much broader range of risks, including emerging threats and vulnerabilities.

A risk orientation hardwires exposure management into your organizational mindset much more deeply than would happen if you were just running through a series of IT and compliance checklists. A risk focus means not just adopting and enforcing security measures but also conducting regular exposed risk assessments and staying really plugged into the evolving threat landscape.

Focusing more specifically on risk also ensures you're attuned to the consequences of an attack — the kinds of operational disruptions you will endure, the financial losses, the reputational damage. And it helps you really get in touch with what bad actors are after and how they will try to get it.

Gaining Insights from the Dark Side

Some very smart people have some very nefarious actions in mind that could cause a heap of trouble for your organization. The best way to stay one step ahead of them is to consider what your infrastructure looks like from their perspective, from the outside in.

Think about all those headlines about cyber events (we include a few in Chapter 1). It's safe to say that most of them succeeded because someone spotted an opportunity that the victim was not aware of. In each case, the victim was likely making a good-faith effort to build solid defenses and protections. But they didn't think of that one vulnerability off to the side, a door left open — probably not the front door, maybe a side door or a back door, even more likely a door in a totally different place.

TIP

To protect your assets, you need to look at the entire ecosystem, and every single connecting entity. You need scans to enumerate all the assets. But not only that, you need to search for assets in areas you may not even be aware of. You can't start from a known list of divisions and begin scanning. How do you know the list is complete? Depending on your organization, a detailed map of the whole business structure could include hundreds of departments, subsidiaries, and acquisitions. Assets exist not only in your company's name but also in all the brands your company owns. And you must search for these assets, assuming that your list of locations is not complete.

An attacker will pay attention to all these details and look all over the Internet for possible paths of entry. Billions of servers and devices are out there, and any one of them might have unknown and unmanaged assets that could be an entry point.

The attacker we're imagining will be looking for that point, eager to find the path of least resistance. An attack will be planned carefully to avoid any notice. From the attacker's perspective, it's far preferable to roll in via the room service cart than it would be to kick in the door of the hotel room.

And that's the perspective you need to adopt. You've done the IT security equivalent of putting locks on all the doors you know about, installing security cameras, and setting alarms. What have you not thought about? What assumptions have you made that might be incomplete? What are the "unknown unknowns"?

Fighting Fire with Fire

A lot of great information can be learned from the various educational programs teaching IT security. You might not, however, emerge with the insights of an attacker.

It's not only possible but critical to take an "outside-looking-in" approach to your security challenges, automatically noticing vulnerabilities and other security gaps before any attacker does, and doing so continuously to keep up with your living, breathing, growing and changing attack surface.

Just like an attacker, your enterprise can fully understand its assets, map out how they're connected, find the easy paths that attackers will be seeking, prioritize what needs attention first, and fix things before they're exploited. By understanding what approaches an attacker might use on the offense against your enterprise, you can build a much more effective defense.

Chapter 7 provides details on how these types of insights are now working on behalf of clients wanting to secure their external attack surfaces.

IN THIS CHAPTER

- » Getting to know your assets
- » Figuring out what you don’t know
- » Appreciating the value of context

Chapter 3 Understanding What You Own

In Chapter 2, we talked about why you need to think like an attacker to best protect your organization. One of the things an attacker does is thoroughly map your organization and then find a path through assets belonging to each entity. This chapter discusses how to do that, including how to determine what traditional approaches might miss. It also discusses the kinds of details you need about your assets to build context that help assessing and fixing issues.

Assessing What You Know

Your external attack surface encompasses all Internet-accessible assets connected to your network, regardless of their source of location.

To find and catalog your assets, you likely use various techniques and tools such as network scanning, vulnerability scanning, asset management systems, configuration management databases (CMDBs), and open-source intelligence (OSINT) tools:

- Network scanning identifies assets through known IP addresses, ports, and services, while vulnerability management scanning detects weaknesses by comparing devices to databases of known vulnerabilities.
- Asset management systems and CMDBs help maintain records of hardware, software, network devices, and their lifecycle, with CMDBs also storing ownership information.
- OSINT tools gather publicly available information from the internet, like social media and websites, to monitor your digital footprint, identify potential risks, and uncover exposed assets, open ports, leaked credentials, and vulnerable email addresses.

While these tools provide valuable insights into known assets, the critical challenge lies in acknowledging what you don't know. Ignorance can lead to significant risks despite the saying, "what you don't know can't hurt you."

Realizing What You Don't Know

WARNING

Long story short, all that information about your known external exposures is crucial but it's incomplete. There are limitations to rounding up useful data using any of the tools and processes mentioned in the previous section.

Unknown risks

REMEMBER

The fact is, traditional security controls and the people operating them can't give a complete picture of all external exposures. The usual methods just can't find these omissions (or *unknown risks*). There are a number of reasons why.

Looking only at your known assets leaves a gap where something might be lurking. Your organization has assets and vulnerabilities living in the gaps between known assets.

WARNING

Some of your unknown risks come from what's known as *shadow IT* — assets lurking in the shadows, that only a few people are aware of. These can be assets that are perfectly legitimate in nature, deployed on-purpose by your organization, but without the knowledge of your IT professionals.

As mentioned in Chapter 1, it's super-easy these days for a department to unilaterally spin up a cloud environment through a subscription service or SaaS and charge it on the company credit card. This environment may have security controls that are inadequate or nonexistent, but who would know if no one is looking? "What you don't know can't hurt you"? Totally wrong.

Then there's the problem of constant change. Assets change all the time, according to one study, nearly 10 percent of them every month. Even if you could be certain you've covered all the known assets and all the gaps today, a month from now you could be missing a boatload of potential trouble.

Misusing vulnerability tools

Even with all your vulnerability scanners and penetration testing and the like, you still don't know all the security gaps that leave your organization at risk.

Think about how you configure a vulnerability scan. You plug in a target range of IP addresses and the tool goes and takes a look. Want to look somewhere else? You've gotta tell the tool. A 2021 Enterprise Strategy Group (ESG) survey called "Security Hygiene and Posture Management" found that nearly half of organizations don't look for vulnerabilities in SaaS applications, workloads running in public clouds, or third parties.

Another problem is that a lot of tools are not used holistically. A vulnerability management team may spend its time checking off a to-do list of vulnerabilities that represents only a tiny subset of potential exploits.

Building Valuable Context

REMEMBER

Understanding what you own is not just a matter of making a list and checking it twice. Excelling at this task requires gathering and processing a lot of contextual details about your assets. For example:

- **Knowing the organization that owns it:** By starting from a point of understanding the business structure, assets can then be discovered with this context in mind. You then can know if it's a business unit, subsidiary, or branch that's responsible.

- **Device-related data:** That means such things as open and closed TCP/UDP ports, certain software platforms, operating system versions, and connections to other platforms, for example.
- **Technical links to data and services:** You (and an attacker) can learn a lot about business importance by studying the links between machines, hyperlinks, gateways, third-party code, and other kinds of tech relationships.
- **Hard to find vulnerabilities:** Security testing should put the spotlight on issues that won't necessarily show up in a list of common security vulnerabilities — such as broken asset control, cryptographic failures, failures in software and data integrity, and susceptivity to injection attacks, for example.
- **Threat intelligence information:** These would be vendor-provided or open source intelligence solutions, and might include data feeds. Intelligence services aren't necessarily cheap, though.

WARNING

The more you rely on manual processes, the harder it is to discover all the risks and understand external exposures. It's not that manual processes don't work, but rather that they're hard to employ and maintain at scale and at the required cadence.

It's also worth noting that attackers are seeking the path that leads to critical assets, such as payment mechanisms and production databases. That doesn't mean that noncritical assets aren't at risk, though — attackers might target less important assets because they provide a foothold on the way to the real prize.

IN THIS CHAPTER

- **Seeing the shortcomings of existing approaches**
- **Putting an end to time-wasting false positives**
- **Getting the most out of your active testing**

Chapter 4 Embracing the Importance of Testing

Information technology (IT) security experts got pretty good at keeping an eye on things around the perimeter, but then the IT world changed dramatically. This chapter explores how a lot of today's exposures are not spotted by vulnerability scanning. And it spells out why active security testing is the best way to discover threats and vulnerabilities, because manual testing alone can't meet the scale and cadence needed to find and resolve all potential issues.

Finding What Scanning Misses

When your aim is managing external exposures, the idea of scanning sounds like it ought to be pretty helpful. It's kind of like posting guards outside the castle, right? Not exactly.

In fact, though there is certainly a role for scanning, it's likely to do more harm than good if that's all you're doing. It would be like only posting guards at one entrance to your castle and ignoring the back or side gates (or the secret tunnel into the dungeon). Do that and you could lull yourself into a false sense of security, unaware of the gaps. And speaking of false, you'll be pestered with false positives.

REMEMBER

The important point is that scanning for common vulnerabilities and exposures (CVEs) just isn't enough. You need active security testing, and scanning is not the same thing as active testing.

Think of it in terms of a spectrum of thoroughness and helpfulness. Passive scanning includes open-source intelligence (OSINT) tools, DNS scanning, network monitoring, and port scanning. These tools may have zero, or limited, interaction with an asset.

A lot of external attack surface management (EASM) solutions stop at this kind of passive scanning, which is problematic for a number of reasons. With passive scanning, you rely on manually entered IP ranges, resulting in gaps in your asset inventories. And while you get alerts on some common vulnerabilities and issues, you also spend a lot of time chasing down false positives.

REMEMBER

Active testing, on the other hand, taps into an advanced testing engine to put the spotlight on critical external risks to everything from web applications to networks to confidentiality, as well as your organization's reputation. Active testing involves repeated interaction with target assets, far more than passive scanning techniques. Among many benefits, it fills in many gaps, provides more insight about risks, and validates remediations.

Here's the thing: Active testing is a critical part of exposure management but in most cases is beyond the usual capabilities of an EASM tool. A mature exposure management program needs both passive and active ongoing testing of all assets, so it's vital to look for that capability when considering solutions.

Steering Clear of False Positives

It's not like your security team is sitting around with a lot of time on their hands. The last thing they need is to spend valuable time and energy chasing false positives. And yet, false positives are a major possibility if your exposure management solution relies too much on passive scanning. This can happen for a number of reasons.

For starters, passive scanning often makes use of tools such as port scanners, which rely on the initial response presented within a protocol handshake. That's known as *banner grabbing,* but as it happens, banners can be incomplete or incorrect.

The process can make it seem like a vulnerability is present, but it can't validate that vulnerability. Its judgment may be inaccurate — for example, it may not be able to tell if a patch has been installed, or if a system has been rebooted after the installation. Or it may just generate noise, which is a slight euphemism for false positives.

REMEMBER

Whatever the reason a false positive happens, it's a waste of valuable time and introduces alert fatigue, which detracts from real threats.

Gaining the Benefits of Active Testing

While there are several benefits of incorporating active security testing into assessing your risk exposure, the following sections discuss three: high confidence threat finding, reducing upfront work, and adding insights about assets.

Finding really bad threats with high confidence

Active testing evaluates the entire communication session for troubling behavior, rather than just relying on protocol handshake information. It's far more likely to spot a vulnerability or risk on pretty much any digital asset type. Active tests are the only way to provide visibility into many kinds of advanced risk, including susceptibility to SQL injection attacks, reflective cross-site scripting, security misconfigurations, credential stuffing, vulnerable shared libraries, and many more.

It has accuracy exceeding 90 percent confidence when it comes to identifying vulnerabilities. That happens to be the minimum confidence level for assigning human staff to resolve issues.

Reducing the upfront work of red teams and pen testers

Testing everything not only keeps your attack surface far more secure, it also helps inform other areas; for example, prioritizing pen testing and red teaming efforts. It improves the focus of your human security team members, allowing for greater output. It's essentially an automation of the up-front setup work they normally do, which allows them to more quickly get to hacking their target asset and doing so on many more critical assets.

Adding helpful insight about the asset

Active testing helps to bring out the context discussed in Chapter 3. Context is crucial for prioritizing remediation. For example, consider a vulnerability that's on a database server containing PII versus the same vulnerability on a benign server. It's pretty much a no-brainer which one should have the highest priority. Passive scanning won't be able to distinguish that nuance.

The bottom line is, more testing is better. EASM approaches that solely rely on passive scanning have trouble enabling testing with enough frequency and a broad enough scale. Manual work isn't just inconvenient — it's downright inadequate. What you need to find are cost-effective options for better automation so that you can assess 100 percent of your external attack surface.

IN THIS CHAPTER

- Realizing why responses are slower than they need to be
- Deciding how severe a vulnerability really is
- Gauging whether attackers will spot a vulnerability
- Determining whether adversaries will care about specific assets
- Building intelligence about exploits
- Understanding how valuable the asset is (or isn't)

Chapter 5 Establishing Priorities

You know lots of threats are out there, and of course you want to be aware of them all. But if you could really make a full list of the vulnerabilities, you'd probably faint. There's no way you could address them all in a timely manner. The good news is, you don't have to.

This chapter explores what gets in the way of speedy remediation, then runs through the best thought processes for prioritizing risks. It offers ideas for gauging the severity of a vulnerability, learning how discoverable it might be, deciding whether an asset will be attractive to an attacker, and ultimately, prioritizing the risks so you know what to tackle first.

Speeding the Response

A 2021 Enterprise Strategy Group (ESG) study called "Security Hygiene and Posture Management" found that for a large enterprise, the mean number of assets in their attack surface is about 100,000. And, of course, that attack surface keeps growing and changing every day. On any given day, hundreds of security gaps — maybe thousands or even tens of thousands — need to be closed.

One Fortune 100 insurance company's vulnerability scanners flagged as many as 5,000 critical issues at any given time, yet the company could only remediate about 50 a month. Sure, it would be great to remediate every vulnerability the moment you discover it, but that's a dream world for any enterprise. You need to prioritize.

REMEMBER

Before we get into prioritization, though, it's worth thinking about which factors slow down your remediation today. And as a matter of fact, a solid external exposure management program addresses some of these factors:

- **Long discovery times:** The less visibility you have into your external attack surface, the slower your discovery is going to be. If your monitoring and scanning functions aren't up to snuff, your discovery can't keep up.
- **Lack of asset attribution:** The logical first step in remediation is accurately attributing each asset to the responsible team or individual who will do the work. The more assets you have, the more difficult this can be.
- **Lack of risk evidence or validation:** The longer it takes you to prioritize your risks, the longer it takes to get started on the remediation. Risk evidence is vital for prioritization, as the rest of this chapter points out, so insufficient evidence and a lack of risk validation leaves you slow out of the starting gate.
- **Time-consuming fix validation:** The job isn't done until you've validated the fix. If manual verification is required, that delays your ability to check that vulnerability off the list, especially when you have a high volume of vulnerabilities to address.

Ranking Priorities

Now that we've spelled out some of the problems that prevent you from remediating everything everywhere all at once, the only real path forward is prioritization. Your organization must adopt an approach not just for discovering vulnerabilities, but also for understanding which are the biggest concerns right now, and which can wait until later.

TIP

You need a way to establish scores for analyzing, sorting, and ranking risks. A priority score gives the marching orders for remediation, and if all is working well, clearly communicates why certain risks must be addressed first.

A lot of thought can go into scoring, but if you keep these basic criteria in mind, you will be in good shape. Weighting these criteria helps you prioritize risks to your enterprise:

- Business context, which helps put the spotlight on assets that will be especially interesting to attackers.
- Potential impact, both the technical impact and business impact of the exploitable asset.
- Exploitation complexity, which helps you know which vulnerabilities lie upon an attacker's preferred path of least resistance.
- Attractiveness, which considers an attacker's appetite and eagerness to go after an asset.
- Discoverability, which is a consideration of both how easy it is to discover the vulnerable asset and how likely it is that a sophisticated attacker will be able to figure out that the asset belongs to your organization.
- Remediation effort, which ponders how easy or hard it will be to fix the risk.
- Number of vulnerabilities on the same asset, offering more avenues for an attacker to attack.

Understanding context and impact

As you prioritize risks to line them up for remediation, a good first question to ask is, just how severe is this vulnerability? For example, say you have found a security issue on an abandoned or "empty" Apache server. That's probably not going to be all that high on the list because vital data is not at risk.

On the other hand, if you have sensitive business documents stored on an unpatched file server, that's much more likely to be a red alert situation. That's a potentially high-risk vulnerability.

TIP

Here's where you need to bring in all the business context you can while also thinking like an attacker would think. Business context helps you determine which assets are most valuable to your organization from a business perspective, how critical they are to a material business process, as well as where they stand in terms of technical importance.

You can bet that assets you think are valuable will also be attractive to attackers. If these assets happen to show up with vulnerabilities, you quite possibly have a problem.

That said, assessing this question is only part of the equation as you're determining prioritization. That's because there are other factors to consider as you decide just how alarming this situation might be.

Discerning its attractiveness

Thinking like an attacker helps your organization spot attractive targets before an attacker does.

TIP

Attractiveness can be thought of as a triangulation of attributes we just discussed, which we can summarize like this:

- **Easy to find:** We're back to discoverable, which might be as simple as publicly available and easy to get to.
- **Easy to take advantage of:** It's like a car in the parking lot with the windows down; that might invite a crime of opportunity. Some vulnerabilities are just easier than others.
- **Has real value:** What looks like personal or important data or passwords is going to grab attention. It's valuable to you and also them on the dark web.

TIP

In determining attractiveness, it's important to consider exploitation complexity. Remember that attackers are looking for the path of least resistance, the easiest vulnerabilities to act upon.

Seeing how discoverable it is

Looking further at that unpatched file server housing sensitive business documents mentioned earlier. You know attackers are going to be interested in those assets, so the next pertinent question is, how discoverable are these assets?

If you find a vulnerability that an attacker is also likely to find, that's a problem. But if your discovery turns up something an attacker is unlikely to spot, you may be able to bump it down the list.

Here's another way that understanding the business context is useful: It can help you play out any potential attack paths. That puts the spotlight on any danger of reaching valuable assets by way of subsidiaries, suppliers, and other connected business partners.

Gaining intelligence on exploits and threat actors

Seeking intelligence about techniques and exploits attackers are actually using is a great ww kind of approach for tracking potential exploits and threat actors. It's how you can look at your assets through what you might think of as a "street-level" lens.

REMEMBER

Attackers can obtain exploit kits on the dark web, along with other tools, and these days more and more of them are sponsored by nation-states seeking certain kinds of technologies. The thing to realize is, what they're looking for isn't always the kind of prize that you might guess if your security approach relies too heavily on the Common Vulnerability Scoring System (CVSS).

The CVSS is rather simplistic in its scoring, and doesn't consider some of the elements that are so attractive about a lot of today's exploitable vulnerabilities. It also completely misses any business context. Your intelligence also needs to be fully plugged into what government and security agencies are warning about, as well as large vendors such as Cisco and VMware.

REMEMBER

All these considerations weighed together help you prioritize the risks exposed across your enterprise's attack surface. Like we said earlier, most organizations face thousands, perhaps even tens of thousands, of seemingly urgent vulnerabilities, far more than you can ever hope to remediate quickly (if ever). An approach that is rational, programmatic, and automated is the way to prioritize the risks and figure out which truly need quick attention.

IN THIS CHAPTER

- **Adopting a new mindset**
- **Getting the whole team onboard**
- **Collecting the evidence you'll need for remediation**
- **Validating your remediation**
- **Keeping track of your progress**
- **Steering clear of pitfalls**
- **Hardwiring remediation into your processes**

Chapter 6 Remediating Issues

Once you've discovered vulnerabilities and prioritized them, now comes the time for remediation. This chapter offers ideas for how best to make remediation efficient and a less hassling part of everyday life at your organization.

Read on to learn why you have to get people rethinking their views of vulnerabilities and changing their approach. This chapter discusses the importance of broad teamwork in remediation, the evidence you need to gather to provide good guidance for remediation, why context is so critical, why you must validate your fixes, how you chart your progress and avoid the pitfalls, and ultimately, how you hardwire efficient remediation into your processes.

Changing Behaviors

One of the not-always-spoken but underlying messages of the previous chapters is: You can't count on yesterday's exposure and attack surface management technologies. The attack surface is growing and constantly changing, it's huge and complex, and legacy tools and approaches are being left in the dust by attacker sophistication.

REMEMBER

What's needed are better tools and processes, to be sure, and the next chapter gets into that in more detail. But at the heart of it all, long-term success relies on changing organizational behavior. You can't only acquire a product and call it a day. Your organization must change behaviors and attitudes, and recognize that the necessary change involves people, process, and procedures alike.

Think for a moment about how things are now, the status quo, so to speak. Vulnerability management means working through a list of common vulnerabilities and exposures (CVEs) that are classified as "critical" or "high." That seems sensible and has been in the past, but these days it's a challenge for a number of reasons.

For one thing, legacy technologies that uncover these CVEs aren't in touch with such things as an asset's business context, which kind of data is at risk, and how discoverable or exploitable it is. Without that kind of context, cross-functional business partners such as business owners don't always agree that the identified vulnerability is really that big a problem.

WARNING

Meanwhile, as the various players debate these "critical" or "high" priorities, they're overlooking a bunch of "medium" and "low" concerns. And as it turns out, some of those lower-level vulnerabilities connect to exposed credentials or personally identifiable information.

You already know this is a problem. But try going into a meeting with executive leaders and telling them this "critical" issue exposes nothing and thus can be moved down the list, while a "low" CVE is actually a huge issue exposing customer data. How's that going to go over?

Your organization must adopt a new mindset to remediating vulnerabilities, and it must be broadly accepted. Cross-functional team trust is critical, because discovering and fixing vulnerabilities is a team sport (more on that in the next section). Everyone must be following the same playbook.

The good news is, adopting the new mindset together and getting on the same page can help build that trust. And ditching the old ways can help you whittle the remediation list to a more manageable workload.

Working as a Team

Vulnerabilities can be anywhere and impact many different people and numerous parts of the organization. And that's not just different departments in the same company, but also potentially subsidiaries, branches, brands that the organization owns, vendors, and partners.

REMEMBER

The thing is, a path into the organization can begin anywhere on that list, and who knows where else. Fixing vulnerabilities takes cross-departmental coordination, cross-functional cooperation, and hand-in-hand work with people elsewhere.

It's definitely technical people in IT and engineering and security, but likely also nontechnical business owners and management personnel. It takes a whole team of different people in different places to keep vital data safe, working together in a carefully coordinated way.

As the last section noted, now's the time for changing behaviors. The people who have been tasked with vulnerability management aren't accustomed to setting priorities collectively with subsidiaries and branches and a whole host of others, but that's what the job calls for now.

Gathering Evidence and Guidance

Clearly, you can't fix a vulnerability until you discover it. And you can't know which vulnerability to fix first until you gather and evaluate all the context needed to properly prioritize your mountain of identified vulnerabilities. But once you get through all that, the teams tasked with remediating the vulnerabilities would surely appreciate some guidance.

To put it another way, the more homework you can do on their behalf, the more likely they'll finish the job quickly and to your satisfaction. This is true whether your vulnerability management team is bringing the job to an internal developer or an outside entity that you believe needs to better protect an asset.

You're best served if you show up with clear evidence of how the issue was discovered and what it's exposing, whether that's credentials, data, critical systems, or whatever. Whenever you can, back up your need with pertinent threat intelligence reports, risk assessment details, vulnerability scanning, or pen testing reports.

TIP

Better yet, show up with some step-by-step guidance in hand on how to remediate the issue. Send that guidance directly into a ticketing or messaging system and you'll really streamline the remediation process and win a lot of friends along the way.

And, it bears repeating one more time, context-based insights are vital for quickly remediating the highest-impact risks. The best way to identify a potential attack path is figuring out how your IT assets connect with specific organizations that are part of your extended IT ecosystem. Pay attention to previously unrelated IP addresses, devices, apps, and certificates.

CASE STUDY: CONTEXT BUILDS TRUSTING TEAMS

A large state in the US recognized the dangers its population faced should a cyberattack occur against public infrastructure. These span things like higher education institutions and utility companies — important to the state and its population but outside of control of the state. The impact of a data or systems being breached, however, would have catastrophic consequences.

When CyCognito was approached, the state already had an intent to buy an EASM solution from a big-name vendor that they already had a relationship with. Things changed during the POV when CyCognito detected a vulnerability with an Internet appliance used for content control and network security — a device controlled by a city, not the state. The city, however, was surprised — they didn't even know it existed. Can you imagine the push back hearing about a vulnerability on a device they don't think is theirs?

The IT operations manager using CyCognito explained the situation, he said, "I was able to log in, tell him the IP address, and all the details how we found it." This changed the relationship with the city to which they said, "They were more than willing to work with us on future security endeavors."

This incident proves the value of having the right context, as evidence can be used to inform conversations across entities and help gain control of external risk exposures.

That context is then helpful in applying the fix. It's just the ticket for determining asset ownership — who can authorize a fix and who can make it happen — and for offering guidance on how to fix the risk.

Trust but Verify

REMEMBER

Once a fix is applied, you can cross that vulnerability off the list, right? It's tempting, but it's not a good idea. You need to validate the fix is doing what it needs to do. You're better off having a continuous validation process. It serves multiple purposes. First, you confirm that remediation was successful. Second, you make certain that it stays that way.

Measuring Progress

If your organization is like most successful enterprises, you like to keep track of your progress. If you can't measure the benefits of an investment you make — new equipment, new software solution, new hire, whatever — how do you know it was worth the trouble and expense?

TIP

As you upgrade your exposure and vulnerability management, be sure you can prove the value of your efforts through metrics that you track through reports and dashboards. Create reports to share with executives who wrote the check for your solution, tracking how you've improved remediation over time.

The best bet is to benchmark your starting point, set goals, and keep tabs on your progress. Consider releasing regular reports — that's good not just for ensuring ongoing leadership support, but also for maintaining momentum and letting your teams across many locations and entities and departments know that their hard work is paying off.

Avoiding Pitfalls

With any improvement, you hope for the best but watch out for setbacks. Your journey to improve remediation could run into any number of pitfalls:

- **Lack of prioritization:** If you try to determine the most critical vulnerabilities but you haven't gathered and considered the proper context, your to-do list is liable to be in the wrong order. Missing a big deal while wasting time on a nonissue can be a costly mistake.
- **Inadequate vulnerability assessment:** Banner grabbing and other legacy scanning approaches miss many assets and lack critical context. Active security testing gives you a better assessment of each asset, what it connects to, and what an adversary will be able to reach by way of that asset.
- **Delayed patches:** Don't let important patches get stuck in a queue because they look arbitrary or unimportant. Know the impact of lingering issues so you can get them the priority attention they need.
- **Insufficient testing of patches:** Unintended consequences are disappointing. That's why you should test patches in lab environments whenever you can, before deploying them.
- **Poor coordination and communication:** Remember what we said about teamwork. You can't have a well-functioning team unless you keep everyone informed and coordinated and in the loop. That includes your technical experts as well as your business owners.
- **Lack of monitoring and follow-up:** A common pitfall is tossing an issue to a different team to resolve, then failing to revalidate to ensure it was successfully resolved. If it's not resolved, you might need to connect your team with additional resources or uncover a missed step, such as failing to restart a process or reboot a server.
- **Relying on a compliance-focused approach:** This is not to discount the importance of compliance, as it's good and prudent and often required by law. But consider compliance as a baseline rather than an end goal. Focus instead on exposures that put you at risk, not just checking off compliance boxes.

- **Insufficient resources:** You can't get the job done if the budget is lacking. That said, you have to be realistic about resources. As you prioritize what you need to fix, set an attainable goal, determine resource needs, and then advocate for those resources.

Building Better Processes

This circles back to the first point in this chapter. You can't just buy a new tool; you have to change the processes and workflows. You need to automate whatever you possibly can.

Say you've found a dangerous vulnerability in a web app. Would you want to manually re-run scans, consult asset management databases, research who owns the app, and all the various steps it takes to get remediation going? That manual effort can take hours or days, and you're liable to end up having to clean up an incident rather than prevent one.

REMEMBER

Automating remediation processes pays off in speeding up the reduction of risk. Automation helps connect dots that reduces time to remediation from months or weeks down to just days, maybe even hours. That's reason enough, but it also can reduce operational costs — a real win-win.

Another avenue for exploring better processes is finding new workflows and integrations. The more you can make remediation routine and hassle-free, the more you can remediate and reduce risk.

TIP

For example, look for ways to integrate any new solutions with your existing tools. Connect your new approaches for discovering and prioritizing vulnerabilities with your existing remediation tools and ticketing systems. That's how to build a well-oiled exposure management machine.

IN THIS CHAPTER

- » **Building automation into exposure management**
- » **Spelling out the key steps of the process**
- » **Ensuring your success in exposure management**

Chapter 7 Automating Exposure Management with CyCognito

The preceding chapters have painted a picture of just how vital external exposure management is, and how challenging it is because of all the blind spots, the false positives, and the lack of resources needed to validate issues and remediate as needed. You've also gotten some idea of what the answer to these challenges ought to look like.

This chapter gets much more specific about how your organization can really get on top of external exposure management. The answer is not just a dreamy wish list — this chapter offers details on how CyCognito, an exposure management platform, can automate external exposure management in a way that is effective, reliable, affordable, scalable, and easy to deploy.

Automating the Work

Chapter 2 discusses why it's important to think like an attacker — that's how you can gain the best sense of where your real vulnerabilities and security gaps lie, which assets are the most important and at risk, and how attackers might try to reach them.

CyCognito's unique approach operationalizes the "think like an attacker" mindset to better secure clients' IT environments. The idea is to create technology that would operate autonomously and take an outside-in "assume nothing" view of the attack surface. The technology uses techniques similar to what an attacker would to find a weak spot for entry:

- Map an entity and any other entity that connects into it.
- Assess all the entities to enumerate and understand their assets.
- Map all asset connections and search for paths of least resistance.
- Use techniques and entryways that will avoid detection.

By automating this mindset on behalf of the good guys, CyCognito provides visibility and generates vital context about the most critical exposures an organization has that are likely to attract the interest of attackers. It takes deep visibility and precise attribution to automate this work. CyCognito uses machine learning models, natural language processing, and graph data models to get the job done. What it doesn't do is start from a pre-programmed list of IP ranges or domains. Attackers don't have that list, why should your exposure management tool? It just leaves room for gaps.

The challenge is that risk and attack paths can be anywhere, on the most obvious assets you know about, and many more than your IT department has visibility into or even knowledge of. Attackers can find their entry path by way of partners, subsidiaries, branches, and any other place across your organization's increasingly vast IT ecosystem.

REMEMBER

That's why CyCognito insists on automated, continuous security testing across millions of machines and applications. Somewhere, critical attack paths — and paths of least resistance — lead to your data and networks. External exposure management is essentially a race to see who finds those paths first: you or your adversaries.

Making Exposure Management Happen

The CyCognito platform boils this important work down into five key categories of work. Here are some of the specifics.

Discovery

This is the task of organizational reconnaissance and discovery; dynamically building a map of your organization and then systematically uncovering assets that are distributed within it. This is your external attack surface. Once the assets are discovered, the CyCognito platform uses a graph data model to visualize and map how they all are related. You have to understand those relations fully, because they're the potential stepping stones on the attack path.

CyCognito's discovery engine maintains a dynamic asset inventory with a graphical evidence chain, built with the help of natural language processing (NLP) and advanced analysis of open-source intelligence (OSINT). The CyCognito platform automates this process and keeps up with change. Figure 7-1 shows the discovery of the entire organization, including subsidiaries and cloud assets, and all external assets associated with each.

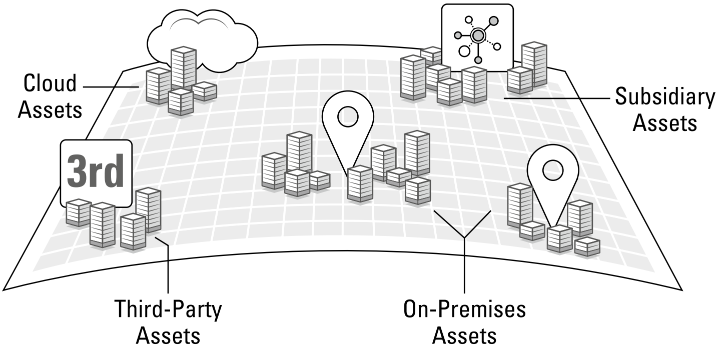

FIGURE 7-1: Discovery maps the organization, including subsidiaries, and the assets associated.

Contextualization

The first step dumps a wealth of information into your lap, but you won't get anywhere if you can't make sense of it. The second step identifies all organizational owners and classifies and attributes all assets. Attribution, in other words the organization that owns the asset, is one of the most important. You can't easily remediate an issue if you don't know who it belongs to.

The point is to close the gaps in knowledge and record-keeping, and add in extremely pertinent business context about potential risks. The CyCognito platform goes beyond common vulnerabilities and exposures (CVEs) to understand what attackers are seeing in your attack surface.

Active security testing

We're not talking about passive scanning, but rather full diagnostic sweeps across the entire attack surface. Active testing pinpoints any security gaps and helps you find data and apps that should not be exposed.

The CyCognito platform brings security testing that is scalable, continuous, and comprehensive, across the full inventory of assets. It's testing it all, not just a fraction of externally exposed assets. And it's going far beyond identifying CVEs. Figure 7-2 shows how CyCognito finds exposed risks across the organization.

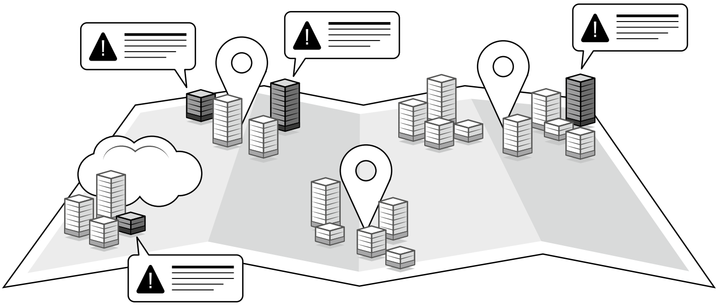

FIGURE 7-2: Exposed risks can be present across the organization, at subsidiaries, and more.

Prioritization

Again, the preceding steps generate a boatload of information about security gaps and vulnerabilities, but they're not all equal. Not in the least. Some need attention immediately; some are not a big deal. This is important because most teams, probably yours, don't have time or resources to deal with everything.

The automated risk prioritization process in the CyCognito platform taps into the context that you've gathered to clearly identify what the most immediate challenges are. You end up with a focused game-plan strategy for addressing the most urgent risk exposures effectively. The process eliminates alert fatigue to put the focus on the top 1 percent of the most critical issues in the attack surface.

Remediation acceleration

As Chapters 5 and 6 explain, lots of roadblocks can slow down the remediation process, and you can't afford those slowdowns. This step enabled by the CyCognito platform sends evidence flows and step-by-step remediation instructions directly into existing remediation tools.

CyCognito streamlines and automates the workflows involved in patching vulnerable assets and verifying remediation. It reduces validation time from months to hours, improving mean time to remediation by as much as 88 percent.

Ensuring a Successful Solution

For an automated external exposure management solution to really work, several key things must all happen at once. CyCognito offers all these important characteristics:

- To find unknown unknowns, the process must be done without guidance, inputs, or told where to look.
- It must fully map your organization structure before looking for assets.
- To build trust, the process must be super-precise and evidence-based.

- It must automatically scale as needed for full coverage.
- It has to be easy to deploy and use.
- It must be easy to consume, communicate, and utilize the results. Accuracy is essential, and the noise factor must be low.
- It has to have active security testing across the full asset inventory to find all the real risks. Consider the adage that "risk accumulates where you're not looking."

IN THIS CHAPTER

- Keeping an eye on visibility
- Classifying and attributing assets
- Testing at a good cadence
- Calculating your MTTD and the two MTTRs
- Reporting to the executives

Chapter 8 Eight Ways to Gauge Your Success

If you're reading this book, you're probably giving some thought to how your organization can up its game in external exposure and attack surface management. And if your mind is heading down that path, you realize that it's going to require an investment of time and effort and money.

Most organizations embarking on investments of time, effort, and money want to know their investment is paying off. Certainly the executives want to know, but so does everyone else. Indeed, seeing progress is an important part of increasing buy-in and gaining momentum. With that in mind, this chapter leaves you with important things to consider as you set out to protect your external attack surface and manage your external risk exposure.

- **Maintaining visibility:** How are you staying aware of your Internet-facing assets, regardless of the business unit or regional branch or subsidiary brand that owns them? Can you find them if you don't have the IP address or other information? Do you really know what development teams or marketing teams have deployed? As things change, new things get spun up, or assets go live, how would you find out or who would inform you?

- **Classifying assets:** What do you know about your assets? Do you know what the asset is used for and what it gives access to? Do you know if they have attack vectors exposed beyond CVEs? Also important, how many of them are classified by such things as business importance and purpose? That's vital info.
- **Attributing assets:** Of the assets on your lists, how many are attributed to the proper organization? If you have an issue with an asset, do you know whom to consult for remediation approval, or who will get the job done?
- **Establishing testing coverage and cadence:** Are you testing 100 percent of your assets? Are you testing at a deep level, such as dynamic application security testing and penetration testing? Are you testing on a regularly scheduled interval? Is your scan cadence staying constant or is it speeding up?
- **Learning from your MTTD:** What's your *mean time to discover?* Are you discovering issues quickly enough? This number should go down as your program goes forward. Essentially, if you find a door was left open, how long ago was the last time you checked?
- **Measuring MTTR:** We're talking about *mean time to respond,* which is basically the time it takes to get from the moment of discovery through the initial steps of reacting to an issue. Are you measuring and monitoring your MTTR? Is your MTTR improving? Do you have a solution for automating the prioritization process?
- **Tracking the other MTTR:** Now we're talking about *mean time to remediate*. This is the time it takes to go from discovery to actually getting the remediation completed and validated. Are you tracking MTTR? Are you improving your MTTR? Do you have solutions in place to automate the process? Do you have solutions that can cut down on hours of research?
- **Reporting to executives:** This isn't actually a measurement, but rather what you do with your measurements. What's the point of metrics if you don't share them? Are you sending regular progress reports to executives? Are you proving the effectiveness of your EASM through executive reporting? Are you proving to management that your EASM is working?

CYCOGNITO

RULE YOUR RISK

Meet CyCognito, the revolutionary external attack surface management platform designed to help organizations understand and test their entire attack surface and reduce their external risk exposure in profoundly effective ways.

CyCognito's State of External Exposure Management Report
cycognito.com/state-of-external-exposure-management

Experience the CyCognito Platform
cycognito.com/product-demo

Get In Touch
cycognito.com/contact

DISCOVERY ▪ CONTEXTUALIZATION ▪ SECURITY TESTING ▪ PRIORITIZATION ▪ REMEDIATION

Reduce your external risk exposure

Technology is changing daily, and the risk your organization faces every day changes, too. Web applications, cloud-based infrastructure, SaaS, and remote work — all realities that drive today's fast pace — also expose your organization to external risk. Your organization needs to shore up its attack surface. Taking an outside-looking-in approach helps you see what an attacker sees — and get ahead. This book from CyCognito gives you all the inside information you need to get started.

Inside…

- Adopt a risk-focused approach to security
- Find unknown or unmanaged assets
- How to build an external exposure management program
- Learn to think like an attacker
- Integrate remediation into your workflow
- Avoid roadblocks and other slowdowns
- Determine your program's success

CYCOGNITO

Steve Kaelble is a *For Dummies* author and published in magazines, newspapers, and more. **Rob Gurzeev** is the CEO and co-founder of CyCognito, with expertise in offensive security and was previously CTO of the product department in the 8200 elite intelligence unit. **Dima Potekhin** is the CTO and co-founder of CyCognito, with expertise in mass-scale data analysis and security.

ISBN: 978-1-394-15385-5
Not For Resale

9 781394 153855

for dummies®
A Wiley Brand