Brought to you by:

NetSPI™

Continuous Threat Exposure Management (CTEM)

for dummies®

A Wiley Brand

Discover the benefits of adopting CTEM

Begin your proactive security journey

Find out more about how to start out with CTEM

NetSPI Special Edition

Eric Butow

About NetSPI

NetSPI is the leader in proactive cybersecurity, helping businesses identify, prioritize, and remediate critical vulnerabilities. With solutions like Penetration Testing as a Service (PTaaS), External Attack Surface Management (EASM), Cyber Asset Attack Surface Management (CAASM), and Breach and Attack Simulation (BAS) as a Service, NetSPI delivers actionable insights tailored to business needs. Trusted by top global brands, including 90% of the top 10 U.S. banks and many Fortune 500 companies, NetSPI is headquartered in Minneapolis, MN with offices worldwide.

Continuous Threat Exposure Management (CTEM)

NetSPI Special Edition

by Eric Butow

for dummies®
A Wiley Brand

Continuous Threat Exposure Management (CTEM) For Dummies®, NetSPI Special Edition

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

ISBN 978-1-394-35409-2 (pbk); ISBN 978-1-394-35410-8 (ePDF); ISBN 978-1-394-35411-5 (ePUB)

Publisher's Acknowledgments

Project Editor: Jennifer Bingham
Acquisitions Editor: Traci Martin
Senior Managing Editor: Rev Mengle
Client Account Manager: Cynthia Tweed
Production Editor: Umeshkumar Rajasekhar

Table of Contents

Introduction

Welcome to the world of modern cybersecurity practices using continuous threat exposure management, better known by its acronym CTEM. This holistic, proactive cybersecurity strategy focuses on continuously identifying, evaluating, and reducing both threats and vulnerabilities in an organization's digital environment.

CTEM is seeing rapid adoption and deployment in many companies and in many industries, and this adoption will continue for the rest of the 2020s and beyond. You're reading this because you know you have to modernize your cybersecurity, and you want to find the solution to help you, your security team, and your company protect your online and physical assets.

About This Book

This isn't just a book; it's your field guide to the modern CTEM strategy that's shaping the future of cybersecurity in a world where new threats emerge every day. So, grab your favorite beverage, sit in your comfortable chair, and explore the next level of cybersecurity.

The book breaks down key components of CTEM in a simple and digestible manner. No jargon or complex theories here — you get a simple *For Dummies* guide to help you grasp the essentials of the modern CTEM cybersecurity approach.

Foolish Assumptions

If you're in charge of security for your organization, it's no wonder that you picked up this book. You may have a title such as Chief Information Security Officer (CISO) or you may have another IT title like network administrator where security is an integral part of your job.

Even if you're in IT but not your ship's chief of security, read this book to understand current cybersecurity concepts and how

NetSPI technologies help keep your business safe. Hey, if you're leading a group of IT people, share this book and its concepts with your team as a part of an overall discussion about security (kinda like building your own Justice League).

You should also share this book with the owner or CEO of your company, and perhaps other leaders. For example, your sales and marketing folks may like to read this book to help them tell potential customers how your business keeps their data safe and sound. And that could be the key to gaining and retaining customers.

Icons Used in This Book

To make things easier and ensure that you don't miss important details, various icons are used throughout this book. This section tells you what the different icons look like and mean.


TIP

The Tip icon is a small piece of advice that may save you time and make your CTEM journey easier.


REMEMBER

This book covers a lot of details and information, so every now and then you see a Remember icon to remind you of the most important details. When you're reading every juicy detail of the book, the Remember icon just helps resurface some of those tidbits.


CASE STUDY

The case studies provide best practices from organizations that have successfully used CTEM.


WARNING

This icon gives you a heads up about risks you might run.

Beyond the Book

This book can help you discover more about CTEM, but if you want resources beyond what this book offers, check out the NetSPI website that's chock full of information and blog posts about the latest in cybersecurity technologies and trends: `https://www.netspi.com/`.

IN THIS CHAPTER

- Learning why exposure management is important
- Applying proactive security in your organization
- Understanding Gartner's CTEM predictions

Chapter 1
Understanding Exposure Management

You don't need to be reminded that threats to your business are everywhere, because you have to battle the evildoers every day. Like any superhero, you want to have the best tools and fighting techniques at your disposal.

Just as Batman took care to design and protect the Batcave and its computing systems to thwart crime, so must you use a modern, proactive approach to security to keep your clients and company safe from your own rogues' gallery lurking in the shadows.

This chapter kicks off by showing you why you should care about modern cybersecurity. Then you'll learn why you need to implement it in your business.

Realizing Why You Should Care

You already know about the importance of securing your environment because you use your computer and other devices like smartphones, as well as being on guard against business email scams known as business email compromise (BEC), where cybercriminals

target a business and pose as trusted people or businesses to trick employees into disclosing sensitive information.

REMEMBER

In your organization, your employees use a variety of tools that nefarious people are always looking to exploit. Your job as a cybersecurity expert is to defend against adapting threats and to assimilate new technologies.

Evolving threats

You may have heard about the term *attack surface*, and that doesn't refer to the side of your sofa your cat prefers to shred. In cybersecurity and IT, an attack surface is the total number of potential entry points in an organization's technology ecosystem that one or more attackers can breach. Those entry points include hardware, software, and user interactions like clicking on an innocent-looking email attachment.

What's more, that attack surface is growing including not just external, internal, and end user threats, but also from cloud assets you and your remote workers use. Specific industries also use devices with sensitive data that attackers are always looking to acquire and sell. If you thought of healthcare, pass Go and collect your $200.

The complex technology landscape

Companies use *attack surface management* (ASM) with technologies and services to continuously manage their assets. ASM includes managing physical or digital assets that are owned or used as part of a subscription, such as Microsoft Office 365.

Organizations also use *external attack surface management* (EASM) to monitor, identify, and mitigate vulnerabilities in their external-facing digital assets, such as their website's e-commerce system.

Cybersecurity has traditionally focused on software weaknesses, and you know this notion is as obsolete as Windows 95. It's likely you're already managing all sorts of activities including employees working remotely, people using their phones, and third-party service providers like Amazon Web Services or other cloud providers.

Implementing Proactive Security

With so many computing assets to manage, companies demand cyberthreat intelligence (CTI) and digital risk protection services (DRPS) that deliver value, and solutions are now trending toward integrating CTI, DRPS, and threat exposure management into a *continuous threat exposure management* (CTEM) program.

CTEM is a proactive security approach that defines stages for identifying, prioritizing, and tackling threats before they can be exploited. ASM is gradually being folded into the CTEM program, and demand for CTI and DRPS that deliver clear value has been a primary driver of this trend.

However, this integration is happening gradually. In its 2024 report "Emerging Tech: The Future of Attack Surface Management," Gartner predicted, "By 2029, 80 percent of ASM technologies will have evolved into a solution set to support different stages of continuous threat exposure management (CTEM) programs, from the established focus on visibility and risk prioritization to cybersecurity validation and remediation."

Dependencies and risks

There are plenty of vendors that provide CTI and DRPS, and businesses have had to work with managed security service providers, managed detection and response providers, and consulting services to get the solutions they need.

That is, if they work with just one vendor. With security challenges becoming more complex daily (or so it seems), IT security professionals have had to decide where to focus their efforts.


TIP

Depending on what your organization needs, more than one vendor may be required, and that means the security chief in the organization has to ensure all vendor tools and processes work well together. If vendors and/or the head of security at the organization don't have the skills or resources, that leads to greater risk of exploits that could sink the organization.

Building solutions with confidence

Finding companies that can provide a comprehensive solution isn't easy right now, and the 2024 Gartner report "Emerging Tech: The Future of Attack Surface Management," stated, "New security requirements are presenting the need to implement a preemptive cyber defense focus. This is driving product consolidation and integration to better cover the new risks arising from an expanding attack surface and to adopt a CTEM program."

IN THIS CHAPTER

- Learning about the five pillars of CTEM
- Building the business case
- Lining up CTEM with your security frameworks

Chapter 2
Learning CTEM Fundamentals

Cybersecurity issues pop up regularly in the news, and if you're in the cybersecurity field, you know that life is never boring. However, it can be a challenge to convince the powers that be in your organization to understand the constant risk, because humans are wired for short-term memories and, as Bruce Wayne said in the film *Batman Begins*, people need dramatic examples to shake them out of apathy. In cybersecurity, that dramatic example could end your career, or even your business.

Traditional vulnerability management frameworks are becoming obsolete because of technology's ever-growing attack surface. But there's a new tool you can add to your utility belt: continuous threat exposure management, or CTEM.

CTEM isn't just a fancy acronym. This process is a fundamental shift in how companies like yours manage their security posture. This chapter discusses the five pillars of CTEM that create a holistic cybersecurity solution, how to build the business case, and aligning CTEM with your existing security frameworks.

Exploring the Five Pillars of CTEM

Unlike traditional risk-based vulnerability management (RBVM) that focuses on only identifying vulnerabilities, a proper CTEM program identifies vulnerabilities and three additional outcomes:

- Ongoing monitoring of potential threats
- Process optimization
- Long-term improvements that ensure vulnerabilities are remediated

To realize these goals, CTEM shifts companies from reactive security to proactive security by using five processes shown in Figure 2-1.

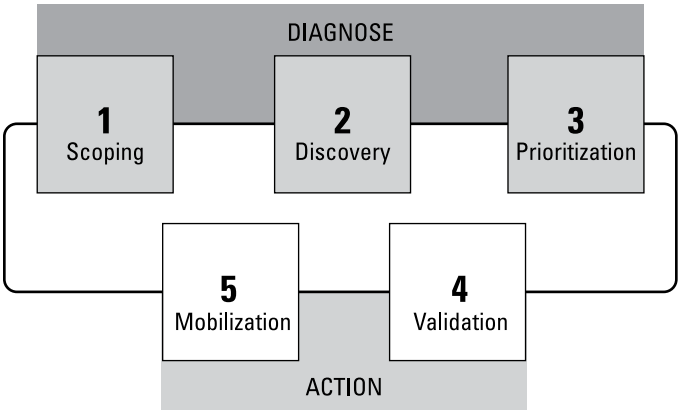

FIGURE 2-1: The five steps to implement a CTEM program.

Scoping process

You won't know what to track if you don't know what assets you have. What's more, you need to know what you want to do, so begin the scoping process by defining your objectives.

Cybersecurity is the business of everyone in the company, so as part of that definition, you need to collaborate with the key players in your organization to discover your sensitive assets and evaluate the potential risks. Then you can align your objectives, your assets, and your current business priorities.

Discovery process

After you have your objectives in place and your sensitive assets catalogued, you need to get a snapshot of how vulnerable those assets are. Penetration testing, which is a point-in-time test that gives you a clear understanding of your threat exposure, is covered in more detail in Chapter 4.

Prioritization process

When you have the results from the penetration test, it's time to triage and categorize your risk levels. At this point, you need to focus your resources on the assets that have the greatest threat exposure. A good rule of thumb when you decide what to fix first is to balance two criteria: the technical severity with the business relevance. If both criteria score highly, that's where to center your attention.

Validation process

You've heard of the old Russian proverb, "Trust, but verify." (Boomers and Gen X kids certainly remember it.) Testing for asset vulnerabilities isn't a one-and-done exercise. You need to retest your vulnerabilities often and, importantly, ensure that your mitigation is effective.

Two ways to do this include running a breach and attack simulation (BAS), which is discussed in Chapter 4, and a simulated cyberattack by ethical hackers known as a red team exercise.

Mobilization process

When the validation process clearly shows one or more assets that have a high threat risk, it's time to put your mobilization plan into effect. You need to track your progress and develop ongoing strategic plans to manage threats, because the rogues never rest.

REMEMBER

Security is the business of everyone in the company, and mobilization really happens throughout the process. You need both training and regular communication so that everyone keeps security top-of-mind and helps you improve CTEM practices to keep your assets safe.

Understanding the Business Case

You already know that CTEM and cybersecurity are musts, but if you're not convinced, there are multiple advantages to using CTEM to stay a few steps ahead of people who can't wait to harm your company and your customers:

- **Maximize security resources:** CTEM's proactive approach prioritizes vulnerabilities and addresses critical threats early, preventing a breach from becoming larger and more difficult to fix.
- **Stay ahead of bad actors:** A Gartner report, "How to Manage Cybersecurity Threats, Not Episodes" from October 2023 noted that "by 2026, organizations that prioritize their security investments based on a continuous exposure management program will be 3x less likely to suffer a breach." This reduction means you'll have fewer bad actors on your doorstep so your security teams will apply much more of their time and resources to addressing breaches that need close attention.
- **Build long-term cyber resilience:** Beyond addressing immediate threats, CTEM's holistic approach doesn't just close security gaps, but it helps prevent similar vulnerabilities from emerging again.

Aligning CTEM with Security Frameworks

So, how do companies use CTEM? They embed CTEM principles using the five pillars discussed earlier in this chapter. Platforms can enable CTEM programs with three out-of-the-box features: penetration testing as a service, attack surface management, and breach and attack simulation.

Three important technologies exist for CTEM:

- **Penetration testing as a service (PTaaS):** In cybersecurity, *penetration testing* (pentesting) is a simulated attack by ethical hackers to identify asset vulnerabilities, exposures, and misconfigurations that unethical hackers can breach.

- **Attack surface management (ASM):** An increasing number of employees are acquiring, modifying, or creating technology without IT's visibility, and this trend is expected to continue growing in the coming years. To govern this ever-growing attack surface, you can use attack surface management, better known by its acronym ASM.
- **Breach and attack simulation (BAS):** CTEM cybersecurity providers also have breach and attack simulation functionality baked into their process so you can uncover any misconfigurations in your system and protect yourself against different types of attacks including malware techniques.

TIP

This is a 10,000-foot overview of the features in a CTEM program. If you want to go deeper, dig into Chapter 4. To see more about NetSPI's offerings, see Chapter 5.

NIST and CTEM: Two cybersecurity superheroes

Imagine cybersecurity as Gotham City, where cybercriminals are like the Joker and Penguin constantly plotting to wreak havoc. The NIST framework and CTEM are like Batman and Robin of your digital defense, each with its own unique crime-fighting approach!

NIST is Batman: The strategically minded, meticulously prepared defender with a comprehensive plan for every possible scenario. He's got his utility belt of security controls, methodically working through identifying threats, protecting the city, detecting criminal activity, responding to incidents, and recovering from attacks.

CTEM is Robin: The proactive, always-on-the-move sidekick who's constantly scouting ahead, finding vulnerabilities before the villains can exploit them. Always one step ahead, continuously scanning the urban landscape for potential threats and ready to mobilize at a moment's notice.

NIST framework: The organized defender

Think of NIST as your cybersecurity drill sergeant. It breaks down protection into five clear-cut stages:

1. **Identify:** Know your digital landscape.
2. **Protect:** Build your digital armor.
3. **Detect:** Keep your radar scanning.

4. **Respond:** Have a battle plan ready.
5. **Recover:** Bounce back after an attack.

CTEM framework: The proactive scout

CTEM is like your cybersecurity ninja, constantly sneaking around and finding vulnerabilities before the bad guys do. Its mission? Stay one step ahead of potential threats. CTEM comprises five phases:

1. **Scoping:** Define your objectives.
2. **Discovery:** Hunt for vulnerabilities.
3. **Prioritization:** Strategically rank and focus on critical risks.
4. **Validation:** Rigorously test your defenses.
5. **Mobilization:** Take decisive action for continuous improvement.

Where NIST and CTEM align in a shared mission: Stopping the bad guys

Both NIST and CTEM have one ultimate goal: protecting your digital kingdom from cybervillains. They're basically cybersecurity cousins with complementary skills. NIST provides a structured, comprehensive approach, while CTEM offers continuous, dynamic threat management.

However, NIST and CTEM align in three ways:

- **Proactive protection:** NIST's protect stage matches CTEM's continuous exposure assessment, and both frameworks emphasize preventing attacks before they happen.
- **Continuous improvement:** NIST's detection and response capabilities perfectly align with CTEM's validation and mobilization processes. Both frameworks love the idea of learning and adapting.
- **Resource optimization:** NIST's comprehensive approach supports CTEM's goal of maximizing security resources. Both help you spend your cybersecurity budget wisely.

Combine for the ultimate implementation power move

Why choose one superhero when you can have two? Use NIST's structured framework as your foundation, then supercharge it with CTEM's continuous, proactive threat management.

MEDTRONIC WORKS WITH NetSPI TO PROTECT ITS NETWORK PERIMETER

CASE STUDY

Building out an incident response team for a global medical device manufacturing company is no easy task, but it is one of Nancy Brainerd's proudest achievements of her Medtronic career thus far.

As Senior Director and Deputy Chief Information Security Officer (CISO), Nancy's primary concern is to defend Medtronic's global attack surface within the constantly evolving threat landscape. To protect patient data and intellectual property, it's critical she knows the size of Medtronic's attack surface, what's vulnerable, and where any blind spots may be.

"It's really important to have a second set of eyes to make sure that you are not leaving yourself vulnerable to attack," Nancy shared. Knowing this, Nancy and her team have been working with NetSPI since 2020 to perform annual penetration tests on their network perimeter, along with spot checking throughout the year to make sure potential threats are not being missed. It's difficult to protect what you don't know about.

With NetSPI's support, Medtronic has been able to define its perimeter, not just once, but in an ongoing fashion, making sure they don't lose sight of systems that might be out there, vulnerable to cyberattack. When looking at the progress of its security posture over the years, the significant thing that has changed is every year the company adds more attack surface to be tested, but instead of the vulnerabilities going up, they're actually going down.

TIP

Think of NIST as your cybersecurity blueprint and CTEM as your real-time threat radar. Together, they create an unstoppable defense system.

Cybersecurity isn't about being perfect. It's about being prepared, adaptive, and one step ahead of potential threats. NIST and CTEM are your trusty sidekicks in this epic digital adventure!

IN THIS CHAPTER

- Evaluating your current security state
- Understanding your organizational roles
- Getting to know your stakeholders

Chapter 3
Building Your CTEM Program

If you decided to start reading this book with this chapter because you want to get started now, take a deep breath. Building a sound CTEM program that will last you for many years needs as much care as building your team and your business.

This chapter starts by taking you through the "before" stage and assessing your current security state. Next, you'll learn how to identify who in your company is responsible for doing what and when. Finally, you'll learn who your stakeholders are so you can report to them on a regular basis.

Assessing Your Current State

One of CTEM's core features is continuous monitoring, so it probably won't surprise you that once you have a CTEM program in place, the amount of data you record and share with your existing security systems will go up dramatically. So, you need to optimize your existing threat discovery and risk management systems first.

WARNING

If you don't optimize your existing systems first, you and your security team will spend most of your time troubleshooting integrations between your existing systems and your fancy new CTEM program. You and your team can be more effective managing your attack surface, don't you think?

But what is an optimized system? The answer is one that is readily scalable. What does that mean? Here are three examples:

- **Replacing a spreadsheet with a risk assessment platform:** A risk assessment platform automates the complete lifecycle of security assessments so that you don't have to track responses in Excel or Google Sheets.
- **Tiering vendors:** Vendor tiering allows you to prioritize critical security vendors so your security team can manage their remediation work more efficiently.
- **Automating vendor risk management notifications:** When you have a risk assessment platform in place, you can set up notifications to track your risk assessment progress and respond to issues quickly.

Knowing Your Organizational Roles

In a severe weather situation, a common mantra is, "Don't be scared, be prepared." Radar and warnings can only take you so far, because if you haven't prepared to ride out a storm and its effects, then your life is in as much danger without a warning.

The same maxim applies when you respond to cybersecurity threats, because panic tends to get you (well, your company) in trouble. So, if you haven't done so already, now's a good time to bookmark this page and create an incident response plan (IRP) with your security team.

What if you already have an IRP? Then now is a good time to review it and make sure it's in line with the data your CTEM program will feed you as well as emerging threats. This is a good opportunity to create a risk-based vulnerability management (RBVM) framework so you can quickly decide if a threat needs to be addressed or disregarded.

REMEMBER

Don't forget to set everyone's role on the security team and what their remediation tasks are. When everyone knows what to do, they can calmly and methodically work through a live cyberattack.

Meeting Your Stakeholders

Speaking of knowing everyone's role during a cyberattack, part of the role of a Chief Information Security Officer (CISO) is to create a cyberawareness training program to address the importance of cyberthreats and vigilance. One topic that likely popped into your mind is the threat of an unknown file attachment in an email message.

TIP

Another role of a CISO is to generate regular cybersecurity reports, and that's a feat. These reports not only keep your company owner (or CEO) and the board of directors (if any) in the loop, but you can share this data with other important stakeholders.

If you're scratching your head, consider sharing your reports with your financial director to see the return on investment as well as your sales and marketing team so they can tout the company's commitment to data security.

Oh, and these generated reports reduce your administrative workload, too, so you can spend less time formatting and more time crimefighting.

IN THIS CHAPTER

- Learning about CTEM technologies
- Using penetration testing as a service
- Running external attack surface management
- Managing the cyber asset attack surface
- Identifying risks on external-facing assets
- Simulating breaches and attacks

Chapter 4
Taking a Tour of CTEM-Enablement Solutions

Many of today's security solutions are reactive. They focus on the latest breach that happens in the news or events in general. Once the word is out about a potential threat, or an actual cyberattack comes upon the company, the security team reacts and it's a stressful time for most people in the company.

The cybersecurity mindset is finally changing because people have realized the attack surface continues to expand at a break-neck speed. Companies continue to buy tools to stay ahead of the game, but often they don't have time to manage them because they're too busy thwarting attacks.

You already know that you want a better way, and that's why you're holding this book. This chapter takes a deeper dive into continuous threat exposure management (CTEM). It starts by taking you from traditional threat hunting to proactive threat management with CTEM. Then it discusses the various tools used

by CTEM including penetration testing and external attack surface management. Next, you'll learn how to manage the internal attack surface, and the chapter ends by talking about simulating breaches and attacks to ensure safeguards are working as planned.

Learning All About CTEM Technologies

The CTEM strategy was introduced by the research and advisory firm Gartner in July 2022 as a proactive approach to cyberthreat management.

Cybersecurity vendors have recognized that the growing breadth of attack surfaces meant companies need much better cybersecurity discipline. The key to that discipline is a proactive approach through what's called exposure hunting.

REMEMBER

That is, a CTEM system proactively searches for weaknesses in your security policies and detects obscure attack vectors such as domains linked to vulnerable servers, end-of-life software that has little to no security updates, and unmaintained web pages.

Cybersecurity providers scan for these security gaps and creative attacks using five tools: penetration testing, external attack surface management, cyber asset attack surface management, digital risk protection services, and breach and attack simulations.

Penetration Testing as a Service (PTaaS)

In cybersecurity, penetration testing (also known as pentesting) is a simulated attack from ethical hackers that checks various portions of your cyberinfrastructure.

These ethical hackers use the same tools and techniques that real attackers may use, and the pentesting process typically has seven stages:

- Defining the scope and goals of the pentest, the systems to be tested, and the testing methods to be used.
- Reconnaissance that helps the testers to understand the target better and plan their attack accordingly.

- Testing of various assets including web applications, network infrastructure, mobile apps, and physical security measures.
- Vulnerability analysis to identify potential weaknesses in an organization's systems, networks, and applications.
- Exploitation, where the testers use the analyzed vulnerability to gain unauthorized access and control of the organization's sensitive data.
- Manual testing for vulnerabilities that automated tools may miss, such as flaws in business logic, authentication and authorization issues, or exploiting existing functionalities for malicious activities.
- A detailed report that outlines the vulnerabilities found, their potential impact to the organization, and recommendations for remediation.

External Attack Surface Management (EASM)

External attack surface management (EASM) combines human intelligence with a variety of tools to identify and validate assets on your external attack surface, which contains all your public Internet-facing assets such as websites, applications, and servers.

Key features of a top-tier EASM solution include:

- **Asset discovery:** The solution must include autonomous detection capabilities to identify all exposed assets across various environments.
- **Business context analysis:** The solution must report which business segment, subsidiary, and/or third-party company is linked to each exposed asset.
- **Categorize exposed assets:** The solution can categorize assets using criteria such as platform and service type.
- **Real-time notification:** The solution must offer both automated and prioritized risk notification as well as remediation recommendations.

- **Integration with related tools:** EASM solutions that are integrated into a single platform with complementary solutions, such as PTaaS, provide more holistic testing outcomes from shared insights. This is a feature of NetSPI's Platform, but it isn't always the case with every EASM solution.

REMEMBER

These five features combine to improve organizational efficiency by reducing manual labor and eliminating redundant IT expenses to reduce costs.

Cyber Asset Attack Surface Management (CAASM)

Cyber asset attack surface management (CAASM) is a solution that equips both your security and IT teams with a comprehensive view of all your digital assets that could be exploited by bad actors. For example, a company has cloud-based systems as well as the identities of users and accounts that could be hacked.

CAASM takes a defender's point of view from the inside looking out by aggregating data — collecting, ingesting, and deduplicating it — to identify potential exposures and coverage gaps across your entire asset landscape, including risks that relate to your interconnection between assets.

With this data at your fingertips, you and your security team can pinpoint weaknesses in your existing security measures, triage priorities, and focus on closing the gaps that pose the greatest threat to your company and your customer data.

Digital Risk Protection Services (DRPS)

Similar to EASM, digital risk protection services (DRPS) focus on identifying risks on external-facing assets such as brand impersonation and data leaks. However, EASM can uncover previously unknown assets, whereas DRPS collects threat intelligence from

multiple sources, including clear (surface) web, deep web, and dark web to identify potential threats to an organization.

Key use cases of DRPS include:

- Proactive monitoring across multiple digital channels
- Comprehensive threat intelligence
- Real-time detection and response capabilities
- Protection of brand reputation, financial assets, and intellectual property

Breach and Attack Simulation (BAS)

A breach and attack simulation (BAS) allows you to create your own tailored simulation playbooks so you can:

- Test detective security controls, processes, and procedures
- Fine-tune organizational security controls
- See your security return on investment

BAS-as-a-service includes dashboards mapped to the MITRE ATT&CK framework to illustrate which phase of the cyber kill chain poses the most risk. BAS supports your CTEM program in the validation and mobilization phases by testing your environment against specific threat actors, malware techniques, and ransomware techniques.

Organizations use many security tools to identify threats such as EDR, SIEM, SOAR, XDR, and MSSP solutions. However, due to time and resource constraints, these security tools often are not tuned effectively. (If you're thinking of your favorite cringing meme after reading that, that's why you're reading this book.)


TIP

Consolidating PTaaS, ASM, and BAS into a single platform brings the most value by optimizing your use of the tools and providing more details on the importance of findings. See Figure 4-1.

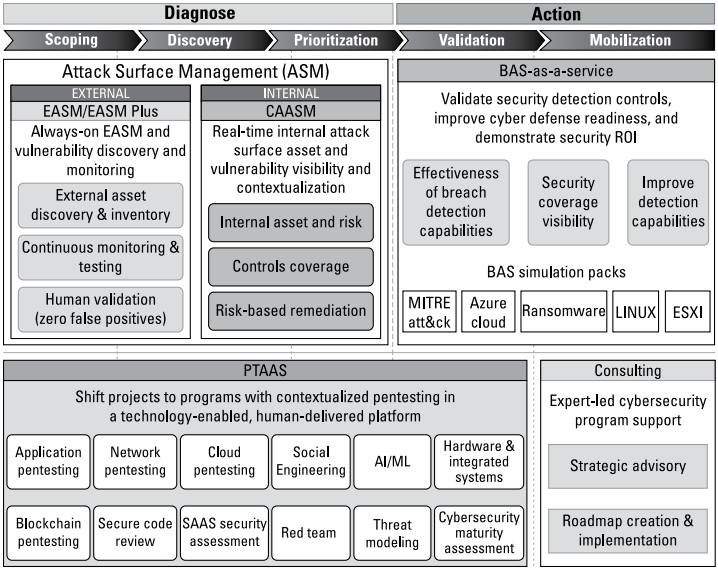

FIGURE 4-1: CTEM enablement is composed of PTaaS, ASM, and BAS.

RED TEAM OPERATIONS

Another common feature of modern cybersecurity programs is running simulated attacks in a red team exercise. Red teams aim to gain unauthorized access to your environment while avoiding detection and maintaining access to test your incident response team's ability to identify and respond to threats. A red team testing exercise uses penetration testers, social engineering tactics, and red team tools to help assess your risk to IT assets, benchmark your current security capabilities, justify security investments, sharpen the skills of your team, and improve detective controls against real-world attacks.

Red team operations leverage tactics, techniques, and procedures used by real-world attackers to better understand exposures and your ability to respond to threats. During red team testing, your cybersecurity provider works with you and your team to define the rules of engagement and project objectives to ensure clear expectations are set and met.

IN THIS CHAPTER

- Providing your team with NetSPI tools
- Understanding The NetSPI Platform's features
- Realizing why you need an integrated solution

Chapter 5
The NetSPI Platform: The Smart Approach to CTEM

Traditional cybersecurity technologies can't keep up with your company's attack surface, expanding every day. The pace of change creates a high volume of alerts, draining your team as they sift through everything that needs attention. You know that continuous monitoring is required. This chapter discusses how The NetSPI Platform propels continuous threat exposure management (CTEM) programs forward, serving your business well today and into the future.

If you've come to this chapter wanting to know what NetSPI has to offer you and your company, read on.

Equipping Your Team with the Right Tools

When you use The NetSPI Platform, you're not just given a "some assembly required" box. You get:

- **Proactive security and continuous monitoring:** NetSPI empowers your organization to continuously uncover, manage, and mitigate vulnerabilities.

- **Deep expertise in testing:** NetSPI's customers trust them for their specialized cybersecurity skills in areas like red teaming, cloud security, AI and machine learning (ML), large language model (LLM) benchmarking, and more.
- **Unified technologies in one platform:** The NetSPI Platform offers cross-functional use cases, giving your organization a streamlined solution that enhances your security and gives you more peace of mind.

Taking a Tour of the Solutions

Before you adopt The NetSPI Platform, you need to understand what the features are so you can share them with your security team and company leaders. The NetSPI Platform has core proactive security solutions, and here are the things to know about each one.

TIP

These solutions are also discussed in Chapter 4.

Penetration testing as a service (PTaaS)

NetSPI offers expert-delivered penetration testing (pentesting) with real-time, in-platform reporting. This results in:

- Decreased detection and remediation time
- Easy integration with your existing ticketing systems
- Meeting your security compliance requirements (such as ISO27001)
- Remediation guidance to resolve vulnerabilities and upskill your team

NetSPI PTaaS delivers a robust pentesting program that includes more than 50 types of pentests. The NetSPI Platform contextualizes outcomes in real time and integrates with your existing security tools so you can quickly close gaps.

NetSPI offers pentesting and proactive security services in several areas:

- **Applications:** NetSPI application pentesting services identify, validate, and prioritize security vulnerabilities in your web apps, mobile apps, thick client apps, virtual applications, and Application Programming Interfaces (APIs).
- **Cloud:** NetSPI cloud penetration testing services identify vulnerabilities in your Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) cloud infrastructure.
- **Network:** NetSPI network penetration testing services identify, validate, and prioritize vulnerabilities on internal, Internet-facing, and cloud-based IT infrastructure.
- **SaaS:** NetSPI's software-as-a-service (SaaS) pentesting includes security assessments for Salesforce and Microsoft 365.
- **Hardware and integrated systems:** This pentesting finds security vulnerabilities that could put your Internet of Things (IoT), ATMs, automotive technology, medical devices, operational technology, and other cyberphysical systems, hardware, and embedded devices at risk of a cyberattack.
- **AI/ML:** AI/ML pentesting identifies, analyzes, and mitigates the risks associated with adversarial attacks on your machine learning systems.
- **Blockchain:** NetSPI's blockchain pentesting service identifies and addresses people, process, and technology gaps across deployments. In addition to testing smart contracts and cryptocurrency, NetSPI evaluates the full spectrum of enterprise deployment models, including private, permissioned, consortia, and public.
- **Secure code review:** NetSPI security experts review source code manually to identify vulnerabilities in underlying frameworks and libraries that are leveraged to build the application and identify any known exploits such as complex injection attacks, use of weak or improper encryption techniques, insecure error handling, authentication, and authorization issues.

- **SaaS security assessment:** NetSPI leverages automated and manual testing methods developed from years of industry-leading application, cloud, and other security assessment types to test Salesforce, Microsoft 365, and more.
- **Red team operations:** These simulated attacks enhance your team's safeguards against threats. Put your security controls, policies, incident response, and cybersecurity training to the ultimate test. See Chapter 4 for more on red teaming.
- **Threat modeling:** Take a holistic approach to identifying potential threats to your company's systems and applications, providing actionable information that enables stakeholders to make strategic decisions.

  NetSPI uses a six-step threat modeling process:

  1. Define security objectives
  2. Information gathering
  3. Environment decomposition
  4. Threat analysis
  5. Countermeasure identification
  6. Reporting
- **Cybersecurity maturity assessment:** NetSPI helps elevate your cybersecurity stance, protect your information, and scale with business growth. They bring a strategic approach to maturing your security program.

You're not left alone on an island to figure out what the outcomes of a test mean; NetSPI's experts provide detailed guidance on prioritization and classification of risk. Plus, after your team remediates the vulnerability, your NetSPI team retests to verify that the gap is closed tight.

REMEMBER

NetSPI works with you to ensure that your cybersystems can fend off real-world attacks.

Attack surface management (ASM)

To govern the ever-growing attack surface, you can use attack surface management, better known by its acronym ASM. NetSPI ASM has two technologies that work together to give you a complete

view of your attack surface: external attack surface management (EASM) and cyber asset attack surface management (CAASM).

REMEMBER

So, what's the difference between EASM and CAASM? While EASM can better inform the scope of external assets, CAASM focuses on internal assets. Both technologies share the capability to overlay vulnerability information to help with prioritization of remediation efforts. When you use them together in The NetSPI Platform, you get a holistic view of your attack surface. This helps make the shift from reactive security to proactive security.

NetSPI ASM significantly supports the scoping, discovery, and prioritization processes with these features:

- Identifying and inventorying visible and hidden assets and vulnerabilities
- Mapping attack paths
- Deep contextual insights for streamlined remediation

NetSPI ASM also sports always-on monitoring and real-time asset and vulnerability updates for continuous exposure validation.

External attack surface management (EASM)

The NetSPI Platform has always-on external asset discovery and monitoring out of the box. This means your organization can eliminate noise (like false positives) with validation. You'll also receive deep context about current attacks with potential attack path scenarios so you can prioritize the attacks to address.

NetSPI security experts manually test and validate findings so you gain visibility into previously undiscovered company and third-party assets. After discovery, NetSPI works with you and your security team to prioritize vulnerabilities and define step-by-step remediation efforts.

Cyber asset attack surface management (CAASM)

The NetSPI Platform gives you total internal asset visibility and contextualization. Here's what that means:

- **Get a holistic view.** You get a map showing your vulnerabilities and real-time centralized risk. You also get a complete

asset inventory that updates in real time as you add, change, or remove assets from your environment.

- **Discover gaps.** NetSPI CAASM identifies security gaps and inconsistencies in real time, as well as severity and risk scoring for each asset.
- **A comprehensive risk picture.** You get a complete internal attack surface report that identifies compliance, governance, and audit gaps.

Breach and attack simulation (BAS)-as-a-service

The NetSPI Platform allows you to test your defenses by simulating real-world attacker behaviors. NetSPI works with you to validate the results so that you have three key pieces of data to act upon:

- You know which security controls work and which ones don't.
- You have the data to fine-tune your security controls and optimize your security stack.
- You know where you need to strengthen your ransomware protection.

NetSPI BAS-as-a-Service executes focused attack simulations in a safe environment to determine whether you have gaps or misconfigurations within your security controls, response processes, and procedures.

In some ways, it's like coaching a sports team. You can run plays to guard against specific opponents and/or malware techniques. After you run your plays, you don't go into a locker room, but you and your team do meet with NetSPI's security experts to identify and fix problems with your game plan.

NetSPI BAS provides step-by-step instructions to test, retest, and close security gaps, but even with all this functionality, you don't have to do this alone. NetSPI security experts will work with you to provide the context you need when the simulation finds gaps

and recommend how to prioritize your risk levels. Once you're set up, you can track your progress in remediating threats over time and show the powers that be that their money fighting the bad guys is well spent.

Understanding the Benefits of an Integrated Solution

The NetSPI Platform is an integrated software-as-a-service (SaaS) solution that consolidates all of the features described in this chapter in a single interface. From that interface, you can:

- Establish an accurate asset inventory
- Identify your exposures
- Evaluate and prioritize risks
- Manage your vulnerabilities
- Validate your security controls
- Proactively improve your cybersecurity stance

In sum, The NetSPI Platform and its security experts can help you confidently embrace rapid innovation while safeguarding perhaps your company's most valuable asset: your customers' trust.

IN THIS CHAPTER

- Understanding the advantages of proactive risk management
- Learning the benefits of an enhanced security posture
- Knowing how a CTEM program lowers costs
- Realizing why CTEM is a future-proof security approach

Chapter 6
Ten Benefits of Implementing a CTEM Program

Upgrading your company to a modern, advanced cybersecurity strategy with The NetSPI Platform and continuous threat exposure management (CTEM) is the way to manage your attack surface now and for years to come. If you're not sure, you need to convince your team, or you need to convince your company leadership, this chapter summarizes the ten benefits of implementing CTEM in your company.

Proactive Risk Management

The C in CTEM is for "continuous," meaning that The NetSPI Platform is constantly on the lookout for vulnerabilities to fix. Even so, this doesn't mean you'll have to react to every vulnerability. You'll receive real-time information about new exposures and how affected assets are connected to your systems so you can decide which alerts need a quicker response.

Improved Attack Surface Visibility

With The NetSPI Platform, you start by scoping your organization's attack surfaces, which are potentially vulnerable entry points and assets. Your attack surface extends beyond the focus of typical vulnerability management programs such as traditional devices and apps, but into the realms of less tangible elements such as corporate social media accounts, online code repositories, and integrated supply chain systems.

After you scope your attack surface, you may be surprised to find potential points of entry that you may never have considered!

Improved Threat Detection

The benefit of continuous threat detection in The NetSPI Platform is that you can detect threats more quickly according to your response plan instead of having to drop everything, put on your snazzy superhero costumes, and fight a threat when it comes in.

Once you receive notice of a threat, The NetSPI Platform helps you confirm that the attackers could actually exploit a vulnerability. If that's true, then The Platform analyzes all potential attack pathways to the asset. Finally, it tells you if the current response plan is fast and substantial enough to protect your business.

Enhanced Security Posture

The goal of CTEM and The NetSPI Platform is not to fix every single security issue, but to give you better data to prioritize those issues. The Platform prioritizes threats based on the following factors:

- Urgency
- Security
- Availability of compensating controls
- The level of risk posed to your organization

The NetSPI Platform helps you identify the high-value assets to your business and focus on a plan of action that addresses them.

Stronger Compliance

It's likely that your team works hard to meet cybersecurity compliance requirements. For example, if you're in health care, you know about Health Insurance Portability and Accountability Act (HIPAA) requirements. Or if you're in finance or e-commerce, you're definitely familiar with PCI DSS, short for Payment Card Industry Data Security Standard.

Your company may also be accredited to the ISO/IEC 27001 international standard that shows your organization's adherence to compliance in all technology environment areas including processes, tools, systems, and employees.

The NetSPI Platform is an essential tool for building and maintaining a resilient and reliable cybersecurity management system that meets all compliance standards.

Faster Response Times

When you implement a CTEM program using The NetSPI Platform, you and your security team will receive continuous findings with data you can use to:

- Reduce delays in operational workflows and remediate security gaps.
- Reduce dwell time between the discovery of an attack and remediation, which results in less damage to your business and its data.
- Focus your team's time and effort on those attacks that have been validated as genuine threats.

Reduced False Positives

What's more, you'll work with NetSPI experts to better identify false positives so your team can focus on the attacks that have been validated and prioritized. As The NetSPI Platform and your processes learn which threats are worth your time and which ones are not, your security team won't be as harried and more likely to approach actual threats calmly and methodically.

Lower Costs

CTEM is a program designed to guide your focus toward exposures that actually pose real risk to your business. By using a platform approach to CTEM enablement, security teams can maximize the output of previously disparate tools by consolidating insights into a single user interface. Plus, partnering with NetSPI's security experts for guidance helps squeeze the most value out of your company's proactive security solutions.

Diminished Blast Radius

When The NetSPI Platform gives you a clear picture of your attack surface, you have the ability to limit the damage, which in the cybersecurity biz is called the blast radius. The Platform will tell you what systems, data, and services could be affected by a detected cyberattack, and that means you can put your crime-fighting tools to work quicker and save the day.

A Future-Proof Security Approach

Because CTEM is a proactive security strategy that's on the lookout for threats that appear continuously, you can use The NetSPI Platform with your other remediation tools to close your security gaps before new threats arise. That keeps The Platform at the vanguard of your company's cybersecurity well into the future.

IN THIS CHAPTER

- Defining your game plan
- Cataloging your technology
- Hunting for threats and closing the gaps
- Teaming up frameworks
- Learning and improving

Chapter 7
Ten-Step Checklist to Implement Continuous Threat Exposure Management (CTEM)

You may have flipped to this chapter because you want to cut to the chase and figure how to implement a CTEM strategy in your business. The ten steps in this chapter serve as a good checklist for you to ensure that you've implemented that system correctly, but it's not meant to provide you with a comprehensive understanding. Within each step, is a brief summary of what you need to know as well as a reference to chapters earlier in the book to learn more.

By following these ten steps, you'll be well on your way to building a CTEM program that protects your organization like a high-tech, proactive superhero shield. Stay ready, stay secure, and you'll never forget to save the day!

Define Your Game Plan

Imagine you're assembling a superhero squad to save your digital universe. The first step is knowing what you're up against.

REMEMBER

If you need to convince the powers that be that CTEM is a sound business decision, that's broken down in Chapter 2.

Sit down with your security team and map out your cybersecurity goals. Pinpoint your most precious assets and figure out where the bad guys might strike. Voila! Now you have a plan.

TIP

If you're a Chief Information Security Officer (CISO) reading this, don't forget to at least ask your company leadership if they want to participate in the planning. Some leaders may want to, others may leave it to you, but it's likely you'll get brownie points for thinking of them.

Take Roll Call for Your Tech

Once you've drawn up your game plan, it's time for a digital head-count. Get your department's Batman to sleuth for the following:

- Every gadget used by everyone in your company.
- Every cloud account your company uses.
- Every app everyone uses on every gadget.
- Every website everyone in your company accesses from their work computers.
- The third-party tools or that vendor platform someone signed up for last year.

The rule of thumb is if it connects to your network, it makes the list. After all, you can't protect what you don't know exists!

Go Threat Hunting

Now that you know what you have, it's time to figure out where the holes are in your digital fortress. To do this, you need to bring in ethical hackers to break into your system before the real

baddies can, because the good guys will use the same tools the bad guys do.

Companies that offer security solutions use methods including penetration testing, or pentesting (discussed in Chapter 4), which identifies vulnerabilities in various areas including:

- Applications including web apps and mobile apps
- Cloud infrastructure
- Internal, Internet-facing, and cloud-based IT infrastructure
- Software-as-a-service (SaaS)
- Hardware such as ATMs and medical devices
- AI/machine learning
- Mainframes
- Software source code


TIP

You can also uncover weak spots using attack surface management (ASM), which is a proactive cybersecurity system that is always checking security gaps in all your cyber assets so you can close them. (You'll learn more about two components of ASM later in this chapter.)

In sum, these tools provide you with a safety inspection of your digital fortress. If you want to learn more about what you're inspecting, there's no need to consult the Batcomputer — just bookmark this page and go to Chapter 4.

Triage Time!

Not all vulnerabilities are equal. Forget trying to fix everything at once (you'll go bananas). Instead, rank the issues by considering which systems an asset is connected to and how much risk a breach of that asset could introduce.

You should assign security levels to each threat such as high, medium, and low. How do you know what threat goes in which box? Keep this in mind: Start with the ones that keep you up at night and work your way down.

Double-Check Your Fixes

Here's the deal with repairs, no matter if it's plumbing or if it's cybersecurity: Fixes don't always stick. In cybersecurity, you need to ensure your patched-up gaps are airtight using breach and attack simulations (BAS).

BAS simulates tactics, techniques, and procedures from real-world threats including from the cloud and ransomware. If you want to learn more about BAS and how it can give you peace of mind, read Chapter 4.

Team Up with Frameworks

Cybersecurity doesn't happen in isolation. Your CTEM program should play well with existing frameworks like NIST. When you mix and match CTEM's proactive methods with NIST's structured approach, it's like getting Batman and Robin for ultimate protection power.

Get Everyone on the Same Page

Cybersecurity isn't one team's job. It only takes one person in the company who doesn't know how to operate securely online to cause an unwitting breach.


TIP

So, train everyone in the company to be a defender, from the intern to the C-suite, and hold regular training sessions to keep everyone up to date. What's more, ensure your teams (IT, security, legal) have the same tools and resources, and are speaking the same language, to work as a unified team.

Clean Up Your Toolkit

If your cybersecurity tools don't talk to each other, you're setting yourself and your company up for chaos, and chaos is bad for business. Choose solutions that work in harmony, covering all the CTEM basics like pentesting, ASM, and BAS.

Once you have the basics, think about other arrows you may need to add to your quiver such as cybersecurity maturity assessment, threat modeling, as well as email, phone, or physical security social engineering tests.

Think of this approach as assembling a carefully curated superhero utility belt instead of pockets full of mismatched gizmos.

Keep an Eye Out. Always.

The bad guys never stop plotting and neither should you, but you're only human. That's where always-on monitoring tools like CAASM and EASM come in.

Cyber asset attack surface management (CAASM) gives you a holistic view over your network users, applications, devices, and the cloud. A CAASM solution also alerts you to vulnerable assets and security gaps in your internal network.

External attack surface management (EASM) does what it says: it's always discovering, monitoring, and testing your external assets such as your public website.

CAASM and EASM work together to track what's happening inside and outside your network before things go wrong. (You can dive into the weeds in Chapter 4.) Staying vigilant 24/7 means fewer surprises.

Learn and Improve

Cybersecurity doesn't have a finish line, so regularly review what's working and what's not with your cybersecurity team. Look at results from tests, attacks (hopefully fake ones), and actual incidents to stay ahead of the game. This is your chance to keep evolving and make your defenses better and smarter against cybervillains.

TIP

Though you're probably reporting to company leadership about cybersecurity in your role as a CISO, consider having regular meetings with the entire company to keep them up to date. This can be part of companywide training.

Discover key components of CTEM

Welcome to the world of modern cybersecurity practices using CTEM. This holistic, proactive cybersecurity approach focuses on continuously identifying, evaluating, and reducing both threats and vulnerabilities in an organization's digital environment. CTEM is seeing rapid adoption and deployment in many companies and in many industries, and this adoption will continue for quite some time. This book is your field guide to the modern CTEM strategy that's shaping the future of cybersecurity in a world where new threats emerge every day.

Inside...

- Learn why exposure management is important
- Five easy steps to CTEM
- Evaluate your current security state
- Take a tour of CTEM solutions
- Ten benefits of implementing a CTEM solution
- A CTEM checklist

Eric Butow is the owner of Butow Communications Group. Eric has authored or co-authored 48 books about business, finance, social media, and technology.

Go to Dummies.com™
for videos, step-by-step photos, how-to articles, or to shop!

ISBN: 978-1-394-35409-2
Not For Resale

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.