

The logo for CYCOGNITO, featuring the word in a bold, white, sans-serif font with a small red square to the left of the 'C'. The background is a dark blue, abstract digital graphic with glowing lines and data points.

**CYCOGNITO**

# Exposure Management

**The Definitive Guidebook for the Security Practitioner**

Reduce exposures, build efficiencies and gain global risk visibility by implementing exposure management in your organization.

# Exposure Management and Your Organization

**REDEFINE YOUR VULNERABILITY MANAGEMENT PROGRAM FOR POSITIVE CHANGE**

## Executive Summary

Your organization's digital footprint is vast and growing. Numerous externally exposed assets, both known and unknown, create a broad attack surface for cybercriminals.

Exposure management (EM) proactively identifies and manages your attack surface risks. A mature EM program combined with continuous threat exposure management (CTEM) provides continuous monitoring, active testing, accurate prioritization and prompt alerting. EM enables your team to gain the information they require to remediate vulnerabilities before they are exploited.

To achieve this level of efficiency EM solutions need to be automated and scalable. Through automation, EM frees staff and reduces cross-functional friction, enabling swift and decisive remediation.



### **EXPOSURE MANAGEMENT'S IMPACT IS SIGNIFICANT**

Gartner predicts that by 2026, "...organizations prioritizing their security investments, based on a continuous threat exposure management program, will realize a **two-third reduction in breaches**."<sup>1</sup>

## About this Guidebook

This guide is designed for individuals who want to understand EM and its impact on their organization's vulnerability management programs. Security practitioners will leave with an understanding of how their roles will adapt to EM and where to go for more information.

# Contents

CHAPTER 1	Introducing Exposure Management	1
CHAPTER 2	Acknowledging Legacy Security Gaps	4
CHAPTER 3	Getting Started with Exposure Management	7
CHAPTER 4	Implementing Exposure Management	9
CHAPTER 5	Your Practical Guide to Becoming an Exposure Management Pro	12
CHAPTER 6	Operationalizing Exposure Management for your External Attack Surface	17

# Introducing Exposure Management

## WHAT IT IS AND WHY IT IS VALUABLE

- The Value of Exposure Management
- Key Elements of Exposure Management
- Why Exposure Management is Achievable
- Six Signs You (and Your Team) Need Exposure Management

## The Value of Exposure Management

Exposure management is a proactive approach to assessing and addressing security risks before they can be exploited by attackers. The goal is to reduce the risk of attacks by identifying risk early and closing windows of vulnerabilities quickly.

Automated vulnerability scanners, semi-automated security testing and manual penetration testing are at the core of most vulnerability management programs. Yet external exposures continue to form the majority of an organization's cyber risk.<sup>2</sup> The lack of coordination between these technologies creates gaps in test coverage, frequency and accuracy.

By proactively addressing vulnerabilities, you can significantly reduce your risk of being breached, understand your overall security posture, help make informed decisions about security investments, and improve compliance requirements more effectively than with vulnerability management programs.

With EM, your teams work on meaningful tasks that have the greatest impact on risk reduction. EM can reduce your issue response time from weeks or months to days or even hours.

## Key Elements of Exposure Management

Exposure management follows a framework called continuous threat exposure management (CTEM). Gartner defines CTEM as a five-step cyclical process for discovering, prioritizing, and validating security issues to provide prompt issue response and visibility.



## CTEM Five Steps



### Scoping

Identify business priorities and the risks that would affect them



### Discovery

Discover exposed assets and their risk profiles



### Prioritization

Identify and address the threats most likely to be exploited



### Validation

Confirm how attackers can exploit an exposure, how monitoring and control systems will react, and if the remedies are feasible



### Mobilization

Operationalize findings efficiently with the aim of reducing friction across approval, implementation, and mitigation



## Why Exposure Management is Achievable

EM combines automation and your existing workflows and technologies to scale to your full attack surface.

Some disruption will be necessary to achieve full EM potential, but when approached systematically, the changes should be incremental and achievable. The long-term benefits of EM make the effort worthwhile.

## Six Signs You (and Your Team) Need Exposure Management

Here are six signals that a security organization would benefit from an exposure management program:

### SIGN 1

**Limited visibility into external assets:** Attackers are often successful in exploiting unmonitored external assets.

### SIGN 2

**Concerns about shadow IT:** IT systems and applications that are used without the knowledge or approval of the IT department, also known as Shadow IT, are an unguarded entry point for attackers.

### SIGN 3

**Frequent security incidents:** If a security organization is experiencing frequent security incidents, it may be a sign that its attack surface is too large or complex to manage effectively.

### SIGN 4

**Difficulty complying with frameworks:** Some frameworks, such as PCI-DSS and NIST, require organizations to have a comprehensive understanding of their attack surface.

### SIGN 5

**Large digital footprint or complex supply chain:** Organizations with a large digital footprint or a complex supply chain are more likely to have a hidden attack surface.

### SIGN 6

**High mean time to remediate (MTTR):** It often takes more than 75 days to remediate an external breach despite the CISA reporting that vulnerabilities are exploited within 48 hours of release.

If your security organization is struggling with any of these challenges, then keep reading. EM is likely to help you improve your overall security posture through greater asset visibility and enhanced visibility into risk.

# Acknowledging Legacy Security Gaps

## THE IMPACT OF STATUS QUO IMPLEMENTATIONS

- Challenges with Traditional Approaches
- Vulnerability Management vs. Exposure Management
- Fractional Improvements aren't Enough

### Challenges with Traditional Approaches

Gaps in asset coverage, scan frequency and technology accuracy have become accepted parts of many vulnerability management (VM) programs. IT security staff work harder to offset these gaps, but despite their efforts, it is not uncommon for MTTR to be measured in weeks or even months<sup>3</sup> instead of days or hours.

### Vulnerability Management vs. Exposure Management

Most organizations maintain some form of three technologies: vulnerability scanners, dynamic application security testing (DAST), and penetration (pen) testing. Each is run at different coverages and frequencies.

On the surface, this appears effective. However, it is not uncommon for vulnerability assessments to be run monthly<sup>4</sup> on a subset of total assets, DAST on less than 10% of web apps and pen testing two times a year on the small percentage of total assets deemed "critical." Nor is it uncommon for an organization to have unmanaged external assets make up 30-50% of its attack surface.<sup>5</sup>

Gaps left by these technologies **can exceed 45%**<sup>6</sup>, a surprisingly large number that is corroborated by the high number of critical incidents and overworked IT security staff.

		VULNERABILITY MANAGEMENT			EXPOSURE MANAGEMENT
		Vulnerability Scanning <i>Automated</i>	Web Application Scanning/DAST <i>Semi-automated</i>	Penetration Testing <i>Manual</i>	<i>Automated</i>
Coverage	Known Assets	50-90%	3-5%	1%	99%+
	Unknown Assets	None/Limited	None	None	99%+
Accuracy		Medium/Low	High	High	Very High
Frequency		Bi-weekly to Monthly	Monthly	Annual	Daily/Weekly
<b>Gap</b>		<b>45%</b>	<b>67%</b>	<b>88%</b>	<b>&lt;5%</b>

Significant improvements in coverage, accuracy and frequency can be achieved with the right technologies and a well-orchestrated and defensible automated workflow.

## Fractional Improvements aren't Enough

It is not uncommon to approach VM improvements tactically by increasing coverage by 10-15 percentage points or scanning frequency from monthly to bi-weekly. Unfortunately, with gaps this large a significant improvement in one or even two areas is not enough to meaningfully reduce risk. The result:

- **Imaginary progress:** Working “faster and harder” using legacy technologies and workflows only marginally improves risk management and wears out IT security teams. EM provides the coverage, frequency and accuracy that transform an existing vulnerability program into a sub-5% gap workflow.
- **Continuous fire drills:** VM programs require extensive work to investigate and validate issues prior to remediation. EM automates all discovery, validation and prioritization steps to provide a high-confidence list of issues to resolve immediately.



- **Lack of meaningful metrics:** VM programs are challenging to implement consistently across a global infrastructure and produce narrow, imprecise and inconsistent views of global risk. EM provides a single view into organizational risks and exposures, with clear success metrics.
- **Inaccurate priorities:** VM products lack the accuracy and precision required to confidently assign remediation teams. EM issues are automatically validated and evidence is recorded to allow rapid assessment and confidence in staff assignment.
- **Attrition:** Fire drills and a never-ending list of issues to resolve promote burnout and attrition. EM allows teams to focus on interesting issues that require a human decision. This keeps tedious, manual efforts to a minimum.

Regardless of whether you are part of the security leadership or security practitioner teams, you likely can relate to these challenges.

Doing nothing is not an option. It's time to implement change.



# Getting Started with Exposure Management

## LAY THE GROUNDWORK FOR PROACTIVE SECURITY

- Four Steps to Starting Your Exposure Management Program
- How to Speak the Language of Exposure Management
- Identify Success

### Four Steps to Starting Your Exposure Management Program

Chapters 1 and 2 of this guidebook discussed VM program challenges and the value of shifting to EM. This chapter discusses how to start your EM journey by implementing the following four steps.

**STEP 1**

**Recognize the need for change.**

**STEP 2**

**Assemble a business, IT security, and risk department task force.**

**STEP 3**

**Build a gap analysis.**

**STEP 4**

**Write the business case.**

The first step is the most important but steps 2 through 4 provide the supporting data to bring them on board.

Once the four steps are completed, you will have the approval, insight and data that allow your organization to confidently describe the impact of EM, why you are adopting it, and the path forward to implement.

# How to Speak the Language of Exposure Management

The transition to EM is helped by using the right words to describe the goal.

## WHAT IS EM

Exposure management (EM) is a threat response program that enables rapid and proactive reduction of risk. EM is an evolution of vulnerability management programs and utilizes legacy approaches as much as possible to minimize disruption.

## LEGACY VS. NEW

People, processes and technologies form the building blocks of EM. Comparing the difference between current “as is” and future “to be” for these three components helps communicate the value of EM.

	LEGACY	EXPOSURE MANAGEMENT	ACHIEVED BY
People	Primarily IT security	Representatives from security and business units that manage risk.	A tiger team <sup>7</sup> that expands risk awareness from IT Security to all risk stakeholders.
Processes	Focus on alert management from singular technologies or aggregated through SIEM at infrequent intervals.	Regular cycles of scoping, discovery, prioritization, validation and mobilization.	Adding automated technologies and new workflows for visibility by all risk stakeholders.
Technology	Singular technologies often run at uncoordinated timings and asset coverage combined with some real-time traffic monitoring.	Security technologies that provide high-confidence, validated results at a frequent cadence.	Automated discovery, validation and mobilization, delivered as a service, converts a highly reactive program into a proactive system.

## Identify Success

Defining success is vital in a project of this importance. With EM:

- Success starts early, at the gap analysis stage, providing tangible awareness of the issues at hand.
- Visible success will occur at major milestones, for example after an EM technology is deployed.
- Long-term success will be recognized once meaningful metrics around visibility, exposed assets tested, and MTTR high-severity risks are tracked.



### TIP

Recalculate the gaps presented in Chapter 2 at three, six and nine-month intervals to track improvements.

# Your Practical Guide to Becoming an Exposure Management Pro

HOW TO LEVERAGE YOUR EXISTING SKILLS AND USE THEM AS A LAUNCHPAD FOR EXPOSURE MANAGEMENT

- Your Roadmap to Becoming an Exposure Management Analyst
- Building Your Supportive Community

## Your Roadmap to Becoming an Exposure Management Analyst

Transitioning from a general cybersecurity analyst to an exposure management analyst involves building upon existing skills while acquiring specialized knowledge in certain areas. Here's a breakdown:

- **Understanding of Attack Surfaces:** Deep understanding of what constitutes an organization's attack surface, including external and internal assets, such as networks, systems, applications, cloud services, and endpoints.
- **Vulnerability Management:** Proficiency in vulnerability assessment tools and techniques to identify weaknesses within an organization's attack surface. This includes knowledge of common vulnerabilities and exposure (CVE) databases, vulnerability scanning tools, and penetration testing methodologies.
- **Asset Discovery:** Skills in discovering and cataloging all assets within an organization's attack surface, including traditional on-premises assets, cloud-based resources, and internet-facing infrastructure.
- **Risk Assessment:** Ability to assess the security risks associated with identified assets and vulnerabilities, considering factors such as asset criticality, exploitability, and potential impact on the organization.

- **Threat Intelligence:** Familiarity with threat intelligence sources and techniques for gathering information about emerging threats, vulnerabilities, and attack techniques relevant to the organization's attack surface.
- **Security Monitoring and Incident Response:** Understanding of security monitoring tools and techniques, such as SIEM, IDPS, XDR and vulnerability scanners, to detect and respond to security incidents affecting the attack surface.
- **Compliance and Regulatory Knowledge:** Awareness of relevant industry regulations and compliance standards (e.g., GDPR, PCI DSS, HIPAA, NIS2, Dora) impacting attack surface management, and the ability to ensure compliance with these requirements.
- **Communication and Collaboration:** Strong communication skills to effectively collaborate with stakeholders across the organization, including IT teams, business units, and senior management, to prioritize and address security risks associated with exposures within the attack surface.

By focusing on these areas, a cybersecurity analyst can develop the specialized skills and knowledge necessary to excel as an exposure management analyst.

## Build a Powerful Peer Network

Cybersecurity can be a challenging field, and it's important to have a network of colleagues who you can rely on for support and advice. Here are some reasons why it's important for cybersecurity analysts to build a network with their peers:

### INFORMATION SHARING

The cyber threat landscape is constantly evolving, and new threats emerge all the time. By networking with other analysts, security professionals can share threat intelligence, discuss emerging vulnerabilities, and learn about new defensive strategies.

### ACCESS TO RESOURCES

Sometimes, you might encounter a particularly tricky problem or need a specialized tool to handle a threat. Networking with your peers can give you access to a wider range of resources, including expertise, software tools, and even training opportunities you might not have been aware of.

## PROFESSIONAL DEVELOPMENT

The cybersecurity field is constantly changing, and analysts need to stay up-to-date on the latest trends and technologies. Networking with peers allows them to learn about new tools, attend industry events, and share training materials. This continuous learning is essential for staying relevant and effective in their roles.

## CAREER ADVANCEMENT

A strong network can be a valuable asset when it comes to career advancement. By connecting with other professionals, you can learn about new job opportunities, get referrals, and position yourself for promotions.

Through continuous development of knowledge and skills, you can position yourself for a successful career as an exposure management security analyst. While industry events are a great place to network (see the Skillset Checklist in Chapter 5), other easy ways to get started include participating in online communities, speaking to more experienced peers in your organization, or attending industry meetups in your area.

# Essential Checklist for Implementing Exposure Management

THE PREREQUISITE SKILLS AND KNOWLEDGE TO HELP YOU PREPARE FOR YOUR MOVE TO EM

- Your Skillset Assessment Checklist
- Your Technology Evaluation Checklist
- Your Implementation Checklist

## Your Skillset Assessment Checklist

To help you with your journey in exposure management, here is a list of sites and events where you can build out your skill set.

### DEVELOP TECHNICAL SKILLS

**Familiarize yourself with open-source tools** such as:

- [Spiderfoot](#)
- [Community version of Burp Suite](#)
- [Metasploit Framework](#)

**Practice in Safe Environments** by utilizing virtual labs or purposefully vulnerable systems for practicing penetration testing techniques.

**Consider Capture the Flag (CTF) Competitions**, where you can participate to test your attack surface skills in a gamified environment. [GoogleCTF](#) and [DEF CON](#) are popular events.

## GAIN EXPERIENCE

There are several resources from SANS Institute, such as the [Attack Surface Management Solutions Forum](#).

Participate in open-source security projects like those on the [OWASP Foundation website](#).

Look for volunteering opportunities like those on the [ISC2 website](#).

## STAY UPDATED

Follow these in-depth cybersecurity blogs:

- [Krebs on Security](#)
- [Security Affairs](#)
- [The Hacker News](#)

Follow these cybersecurity websites:

- [Dark Reading](#)
- [Security Week](#)
- [SC Magazine](#)

Participate in online communities:

- [The Spiceworks IT Community](#) is a broad IT community that includes a cybersecurity forum. It's a good place for new security analysts to ask questions and get advice from more experienced professionals.
- [TechRepublic Forums](#) is a broad IT community that includes a security forum. It's a good resource for staying up-to-date on the latest security news and trends.

## NETWORKING OPPORTUNITIES

Connect and network with other security professionals through a variety of ways:

- **LinkedIn groups for security professionals.** These groups can be a good way to connect with other security analysts in your area or industry. You can find groups by searching for keywords such as "information security" or "cybersecurity."
- **Information Systems Security Association (ISSA).** ISSA is a professional organization for information security professionals. They offer a variety of resources for members, including online communities and local chapters.



**Attend regional and national industry events** such as:

- [B-Sides](#)
- [RSA Conference](#)
- [Black Hat/DEF CON](#)

## Your Technology Evaluation Checklist

EM requires investment in technologies that support full automation, full coverage, high accuracy, and revalidation. Create a list of deployed technologies in your organization and review them one by one from an EM perspective to understand if they meet these requirements.

The table below can be used as a template for recording this information.

<b>TECHNOLOGY</b>	<i>Insert your technology name here, for example, Vulnerability Scanning</i>
<b>COVERAGE</b>	<i>Percentage of assets covered by this technology</i>
<b>ACCURACY</b>	<i>Percentage of accuracy for this technology (higher percentage is lower False Positives)</i>
<b>FREQUENCY</b>	<i>Cadence of this technology (daily, weekly, bi-weekly, monthly, quarterly, annually)</i>

<b>EM PHASE</b>	<b>DOES THE TECHNOLOGY AUTOMATE THE FOLLOWING</b>	<input checked="" type="checkbox"/>
Scoping	<ul style="list-style-type: none"> <li>• Establish individual tracts of IT Security focus as they relate to business priorities</li> <li>• Identify infrastructure segments tied to the parent company, subsidiaries, and brands</li> </ul>	<input type="checkbox"/>
Discovery	<ul style="list-style-type: none"> <li>• Identify assets within the pre-established scopes</li> <li>• Uncover risk tied to identified assets</li> <li>• Correlate risk and assets with business impact</li> </ul>	<input type="checkbox"/>
Prioritization	<ul style="list-style-type: none"> <li>• Rank exposures based on risk level, issue severity, availability of exploit, discoverability of asset, etc.</li> </ul>	<input type="checkbox"/>
Validation	<ul style="list-style-type: none"> <li>• Validate identified risk, remove false positives</li> <li>• Assess the likelihood of attacker success using threat intelligence</li> <li>• Estimate the highest business impact</li> <li>• Identify if remediation speed (MTTR) aligns with business needs</li> </ul>	<input type="checkbox"/>
Mobilization	<ul style="list-style-type: none"> <li>• Operationalize remediation via shared communication and data</li> <li>• Identify if automated remediation is possible</li> <li>• Provide remediation steps if manual remediation is required</li> </ul>	<input type="checkbox"/>

Common existing security technologies to be evaluated include:

- [External Attack Surface Management \(EASM\)](#)
- [Vulnerability management \(VM\)](#)
- [Cyber Asset Attack Surface Management \(CAASM\)](#)
- [Application testing \(DAST\)](#)
- XDR, NGFW, [WAF](#), SIEM, endpoint, Web gateway, etc.

Penetration testing should also be evaluated. While it is not a single technology, it is a common part of vulnerability assessments.

Each protection and detection security technology in place today must be evaluated at a high level to assess its contribution to exposure management and its ability to meet automation requirements.

## Your Implementation Checklist

To ensure consistent and effective threat exposure management, establish regular, cyclical processes within your EM program. Each cycle should follow a five-step approach: scoping, discovery, prioritization, validation, and mobilization. This ensures a comprehensive evaluation of threats.

		TASKS TO COMPLETE	<input checked="" type="checkbox"/>
<b>Phase 1</b> <i>Scope Preparation</i>	Define Scope	<ul style="list-style-type: none"> <li>• Identify critical assets, data, and systems. Understand the potential impact of a breach on your business operations.</li> </ul>	<input type="checkbox"/>
	Assemble the Team	<ul style="list-style-type: none"> <li>• Create a cross-functional team with representatives from IT, Security, and potentially Legal and Communications.</li> </ul>	<input type="checkbox"/>
<b>Phase 2</b> <i>EM Process</i>	Discovery	<ul style="list-style-type: none"> <li>• Conduct a comprehensive inventory of all internet-facing assets, including devices, applications, and cloud resources.</li> <li>• Identify vulnerabilities within these assets</li> </ul>	<input type="checkbox"/>
	Prioritization	<ul style="list-style-type: none"> <li>• Analyze discovered vulnerabilities based on severity, exploitability, and potential impact on critical assets.</li> <li>• Consider the likelihood of a threat targeting your vulnerabilities.</li> </ul>	<input type="checkbox"/>
	Validation	<ul style="list-style-type: none"> <li>• Validate the accuracy of your vulnerability assessments.</li> </ul>	<input type="checkbox"/>
	Mobilization	<ul style="list-style-type: none"> <li>• Develop a remediation plan to address the prioritized vulnerabilities.</li> <li>• Clearly define roles and responsibilities for vulnerability remediation and incident response.</li> <li>• Update security policies and procedures based on the findings from the EM program.</li> </ul>	<input type="checkbox"/>

While the EM program itself is focused on proactive risk identification and mitigation, the knowledge gained from this process can contribute to all three positive outcomes: surviving breaches through improved preparedness, minimizing risks by optimizing resource allocation for mitigation efforts, and building long-term resilience through informed strategic planning.

# Operationalizing Exposure Management

**PROACTIVELY REDUCE RISK, DRIVE BUSINESS VALUE, AND FAST-TRACK YOUR EM WITH CYCOGNITO**

- Deploy Rapidly
- Scope Accurately
- Recognize Benefits Beyond Exposure Management
- Ready to Get Started?

## Deploy Rapidly


Full EM rollout can take time. EM rollout is considerably shorter and easier when you start with the right technology choice. Organizations that deploy the CyCognito platform — without other changes — can reach 95%+ EM technology goals for their external attack surface.

## Scope Accurately

CyCognito fully automates EM scoping, discovery, prioritization, validation, and mobilization phases.

CyCognito understands the potential business impact of a compromise is more important than the severity of the threat. With CyCognito you can choose to scope based on hundreds of automatically gathered contextual elements, for example e-commerce web applications, data exposures in a specific geographic region, and risk to cloud infrastructure.





CyCognito allows your organization to translate risk goals into EM scopes and efficiently action them.

## **Recognize Benefits Beyond Exposure Management**

CyCognito, delivered as a service, permits IT Security teams to reduce or even eliminate the labor-intensive work that has caused friction and held back risk management progress.

IT security and business teams are served fully tested, validated issues with clear remediation instructions at the cadence of their choice. The team no longer has to perform:

- Organizational business structure mapping
- Asset discovery and inventory management
- Test development, execution and monitoring
- Investigative reconnaissance work for classification, attribution and evidence collection
- Lengthy validation time to ensure success for remediations

## **Ready to Get Started?**

See how leading organizations benefit from exposure management and secure their assets with CyCognito. Request a [free demo](#) to get started.

Learn more about CyCognito and EM at [www.cycognito.com](http://www.cycognito.com).

## Notes

1. Gartner - Top Strategic Technology Trends for 2024: Continuous Threat Exposure Management
2. Source: 83% of breaches involved external actors, Verizon 2023 Data Breach Investigations Report
3. Source: <https://www.statista.com/statistics/1363099/average-days-to-patch-vulnerability-by-severity/>
4. Source: <https://www.secureideas.com/knowledge/how-often-should-vulnerability-assessments-run>
5. Source: CyCognito research of current customers, 2023
6. Source: CyCognito gap analysis research, 2024
7. Exposure management center of excellence (EMCoE) is described in Chapter 4 of the CISO guidebook.
8. General CoE information is available at [https://en.wikipedia.org/wiki/Center\\_of\\_excellence](https://en.wikipedia.org/wiki/Center_of_excellence), CCoE information at <https://www.gartner.com/smarterwithgartner/execute-your-cloud-strategy-with-a-cloud-center-of-excellence>
9. \$26K cost per incident on average. Source: <https://www.verizon.com/about/news/2023-data-breach-investigations-report>  
\$16.5M\$ cost per breach on average. 100K records X \$165 per record. Source: <https://www.ibm.com/reports/data-breach>

CyCognito is an exposure management company that helps customers prevent breaches by discovering, testing, and prioritizing remediation for your externally exposed assets. To learn more, visit <https://www.cycognito.com/platform>.