XM Cyber

acme

Executive Report: Continuous Exposure Management (CEM)

Prepared For: ACME Inc.
Prepared By: Customer Success Manager
Date created: June 2025

Table of Contents

Executive Summary

Overall Security Score

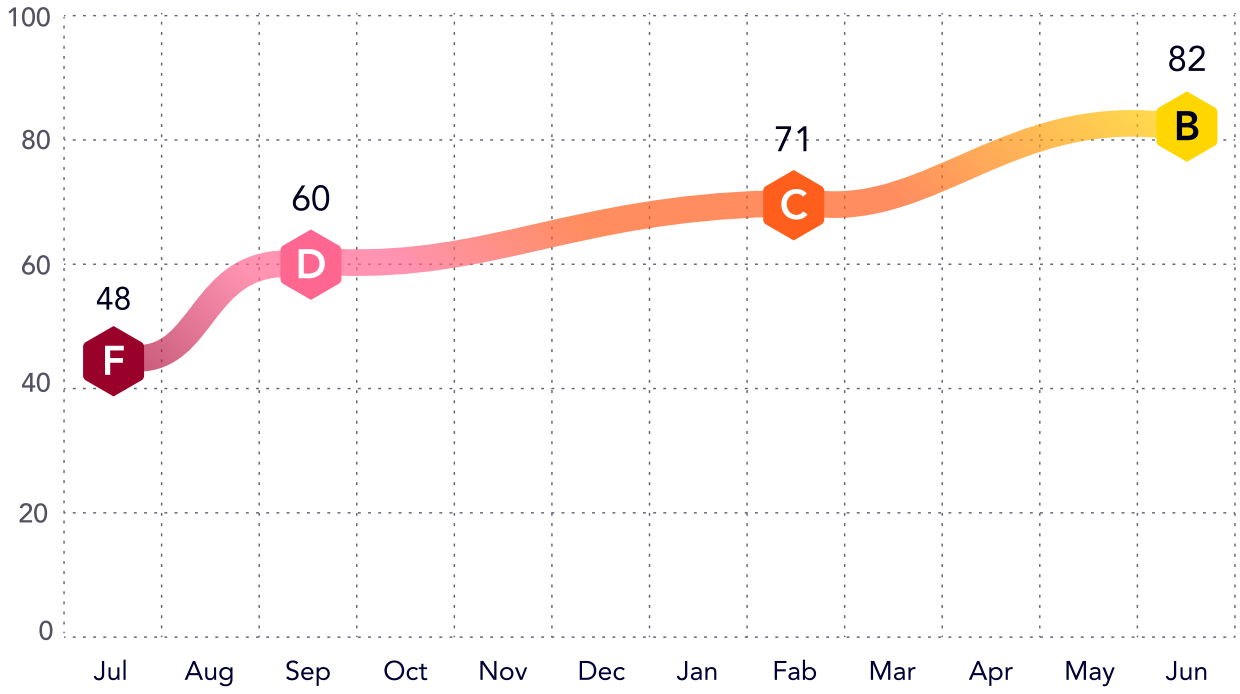
Your security score has been on a steady path of improvement since partnering with XM Cyber. Your team has been focusing on fixing exposures on entities that are in the direct path toward your critical assets. Continuing this path will contribute to a stronger security posture in protecting your key business processes.

Overall Security Score
December 2024

B

82

Overall Security Score Trend



What is the security score?

The Overall Security Score conveys the risk level of your environment by calculating the average security score of every scenario that has been selected. The scenario security score is measured by the number of critical assets that are compromised by an attack path and the complexity of compromising that attack path.

A 90-100 B 80-89 C 70-79 D 60-69 F 0-59

Similar customers in your industry have an average security score of C

Critical Business Processes and Their Security Score

Your Payment System, Customer Data, and Employee Data processes are trending in the right direction, and those processes remain more protected. The Digital Services process continues to improve but is not yet at your acceptable risk level. Your Supply Chain process is severely exposed, which could impact your ability to work with suppliers to continue to serve your customers. Your Customer Services process has dropped from C to D. If this trend continues, you may experience lower Customer Satisfaction scores as your customer services teams will be unable to service your users due to a successful attack against this process.

Payment System

Scenario Security Score

B **85** 80 ↗

% Critical assets at critical and high risk	# Choke Points Critical & High
30% 40% ↘	5 8 ↘

Customer Data

Scenario Security Score

B **80** 78 ↗

% Critical assets at critical and high risk	# Choke Points Critical & High
20% 25% ↘	15 20 ↘

Customer Services

Scenario Security Score

D **60** 66 ↘

% Critical assets at critical and high risk	# Choke Points Critical & High
42% 40% ↗	7 7 →

Digital Services

Scenario Security Score

C **72** 68 ↗

% Critical assets at critical and high risk	# Choke Points Critical & High
30% 35% ↘	4 6 ↘

Supply Chain

Scenario Security Score

F **50** 50 →

% Critical assets at critical and high risk	# Choke Points Critical & High
50% 50% →	9 9 →

Employee Data

Scenario Security Score

B **80** 78 ↗

% Critical assets at critical and high risk	# Choke Points Critical & High
20% 25% ↘	11 14 ↘

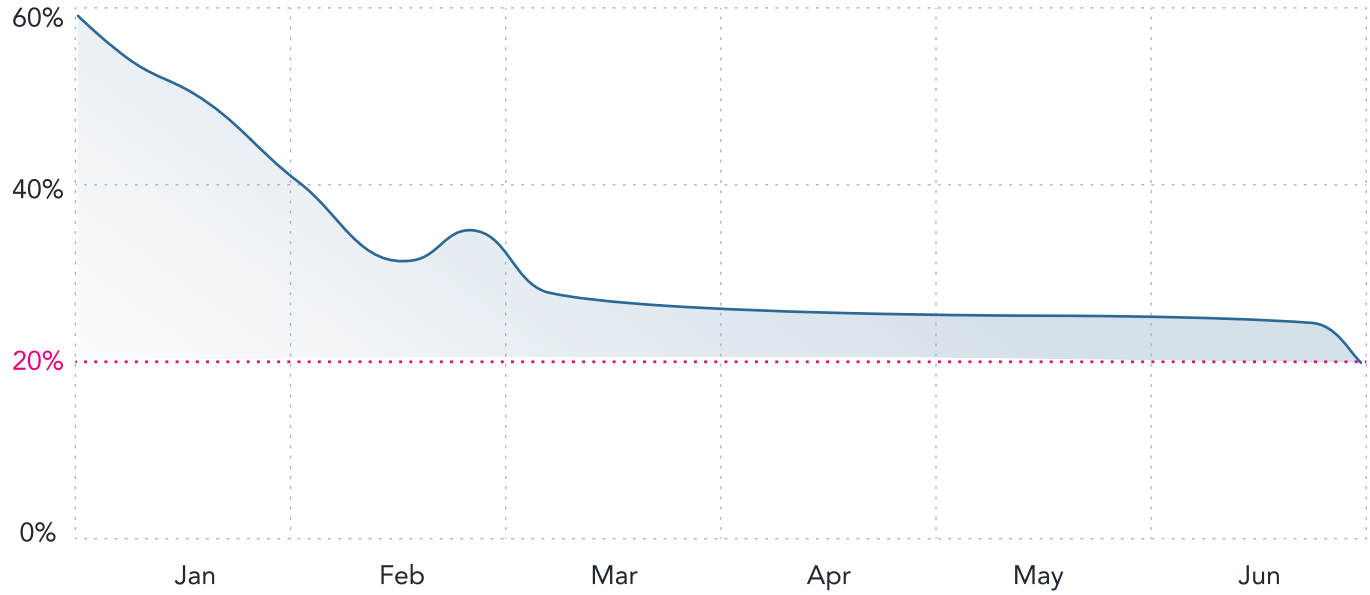
*The scenario cards display the score for this month, as well as the score for last month and the trend (arrow)

Critical Assets at Risk

Overall Critical Assets at Critical and High Risk: 20%

% of Critical Assets at Critical and High Risk Trend

There are 77 critical assets at Critical and High risk in your environment out of a total of 387 critical assets identified (20%). You can also see the distribution of critical assets based on their risk level.



Critical Assets by Compromise Risk Score

Distribution of critical assets based on their compromised risk level

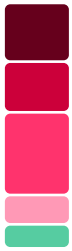
<May 2025>

Total
387

Critical	46
High	51
Medium	125
Low	75
Not compromised	90

<Jun 2025>

Total
387



Critical	32
High	45
Medium	130
Low	85
Not compromised	95

Highest Remediation ROI (Choke Points)

of Overall Choke Points with Critical or High Risk Score: 80

of Choke Points with Critical and High Risk Score Trend

There are 80 entities in your environment that are Choke Points (intersections of attack paths compromising critical assets) which are scored Critical or High. The Choke Point score reflects the number of critical assets it compromises (= blast radius).

Choke Points by Risk Score

Distribution of Choke Points based on their risk score

<May 2025>

Total
639

Critical	38
High	49
Medium	76
Low	237
Informative	239

<Jun 2025>

Total
639

Critical	34
High	46
Medium	78
Low	242
Informative	239

Key Findings

In this chapter you will find the key findings from the XM Cyber Continuous Exposure Management Platform based on what your team defined as most interesting.

Top 5 Critical Assets at Risk

Assess the risk to your critical assets and entities

Entity name	Entity type	Custom + Enrichment Labels	Compromise Risk Score	Compromised since
ATM-Jump-Server	Azure Virtual Machine	Region Northern Europe, RDP Server, Spooler Server	Critical 100%	10/02/2024
PR.AD\dcadm.jacobs	Active Directory User	OT Mgmt	Critical 100%	08/04/2024
global-master-eu	AWS EC2	Public IP, BigFix	Critical 99%	05/03/2025
spectre05_POD	SAP Application	Web Server, PROD-Env	Critical 99%	01/04/2025
CELDEL2086	Device	Device without EDR	Critical 95%	09/01/2024

Top 5 Entities with Highest Remediation ROI (Choke Points)

The number of Choke Points scored critical and high was reduced from 130 when you deployed XM Cyber CEM to 80 based on your team's great work. The Choke Point score reflects the probability of the attacker reaching the choke point and the impact to your environment if this happens. Score calculation is based on risky breach points and the number of compromised critical assets. The higher the score, the more critical it is to fix.

Entity name	Entity type	Custom + Enrichment Labels	Choke Point Score	Critical assets at high risk
Admin units	Azure App	Production, Finance	100	65%
co1manlpy01.prcins.net	Linux, SSH Server	RDP Server, Spooler Server	100	81%
ne7jsslpv71	Linux, SSH Server	intune_management	95	44%
co1jwalpv72	SSH Server	Staging	94	37%
drrtinmo	AWS user	Inactive identity	89	70%

Top 5 Most Impactful Exposures Recommended for Remediation

Exposure	Exposure group	Complexity	Critical assets at risk	Remediation
Taint Shared Content	Vulnerability, lateral movement	Low	35%	Remove write permissions
PrintNightmare - Windows Print Spooler (CVE-2021-34527)	Vulnerabilities, Privilege Escalation	Low	19%	Disable the Print Spooler service
Azure Graph Role Compromise	Azure, Initial Access	Low	23%	Limit which principles have dangerous roles
Text4Shell (CVE-2022-42889)	Vulnerabilities, Lateral Movement	Low	30%	Apply patch from Apache
Domain Credentials	AD, Defense Evasion, Lateral Movement	Low	45%	Remove users from groups

Top Scenarios at Risk

Scenario name	Scenario Security Score	Critical Assets at critical and high risk
Hybrid Risk I On-Prem to DEV	F 13 (13) →	100% (100%)
Ransomware I Clients to backend	F 25 (25) →	97% (97%)
Supply Chain I 3rd party to critical assets	F 50 (50) →	50% (50%)
Exposed Credentials to critical assets	F 55 (45) ↗	95% (100%)
Azure workloads open to the internet	D 60 (50) ↗	89% (100%)
Risky principals to Admin users	F 52 (52) →	65% (65%)

Remediation Overview

This chapter reviews the remediation performed, its impact, and the next top entities and exposures in need of fixing.

Remediations performed over the past month

	Attack Techniques that were Fixed	Impact of Remediation
01	Fixed Azure Add Role Assignment on Ghost-SMB (Azure SQL Server)	Prevent privilege escalation allowing access to employee data
02	Applied patches for OpenSSH on Linux server Millan345	Protect the SWIFT server
03	Activate EDR on kassVM12	Block attack on the shared file server holding client files

Recommended remediation for next month

	Recommended Remediation	Expected Impact
01	Restrict WRITE permission to shared files on Aaron.sepertaf (AWS S3 bucket)	Prevent attackers from compromising sensitive customer data
02	Remove permissions from local group on xyz Linux server	Protect the AS400 payment server connected to it
03	Remove nested groups in your exchange server	Block privilege escalation of non-admin users

Report Scope

The scope of the report determines the calculations of the security score. Changes to the scope will impact the security score. For example: adding entities and introducing new exposure types will uncover risks and reduce the security score, while suppressing scenarios or exposures will result in a higher security score.

June 2025 report scope

Entities

350,000
(monthly average)

Servers

1500 Linux and Windows

Workstations

5000 MacOS and Windows

Azure

1500 Subscriptions

Kubernetes

800 Clusters

AD Domains

ad.acme.com
emea.acme.com

Changes in scope over the past 6 months

+10

new sensors deployed

Extended

Azure

coverage
+200 Subscriptions

Out of Scope

Servers

900

Workstations

3000

XM Cyber

acme

Appendix

Glossary:

Scenario: A continuous simulation of an attacker's lateral movement from a pre-defined breach point to selected critical assets by using a variety of attack techniques including vulnerabilities, misconfigurations, over-permissions, and identity risks.

Critical Assets: The most valuable assets in your environment for your business operations, for your technical operations, or for an attacker looking to profit. These assets are identified automatically or in a joint workshop and can be devices, cloud services, data, or identities.

Breach Point: An endpoint with a high probability of being compromised by an attacker to infiltrate the organization and in most cases the first step of the attacker's lateral movement towards more valuable entities.

Choke Points: Entities that pose the highest risk to your critical assets and environment, and are an intersection of multiple attack paths compromising these critical assets. Remediation of these entities generates the greatest improvement of your security posture.