praetorian

eBook

Continuous Threat Exposure Management (CTEM) and Cybersecurity Insurance

Get Started ›

Inside this eBook

Introduction

Cybersecurity insurance has become a ubiquitous part of the modern security landscape. Over the past five years, cyber insurance premiums have doubled[1]. The global cyber insurance market ballooned to $20 billion in 2024 and is expected to reach $29 billion by 2027[2].

The demand for cyber insurance is driven by an increase in cyber threats. When attack surfaces grow in complexity, new threat tactics and techniques become possible, providing additional paths for threat actors to exploit. In 2024, ransomware continued to dominate the threat landscape, but cybercriminals also increasingly resorted to supply chain attacks, business email compromises, and data breaches[3]. For modern enterprises, cyber insurance is all but a requirement.

Unfortunately, purchasing cyber insurance is not a straightforward process. Underwriters require a wealth of information from multiple sources throughout the organization. Further, industry standards are not as robust as in other types of underwriting, leaving much to the discretion of the cyber insurance underwriter.

This eBook highlights some of the challenges felt by organizations during cyber insurance underwriting and discusses how Continuous Threat Exposure Management can help.

Challenges with Insurance Underwriting

According to a recent report from Woodruff Sawyer[4] about projections for 2024:

56% of underwriters believed cyber risk will increase greatly

50% of underwriters believed underwriting scrutiny will increase

81% of underwriters believed cyber insurance premiums will increase

Insurers are increasingly aware of the growing cyber threat to most organizations. This leads to greater demands from the insured during the underwriting process and higher premiums afterward. Organizations that do not successfully navigate the underwriting process risk unnecessarily high premiums or losing coverage entirely.

Underwriters now ask for more information than can be feasibly provided by one person,[5] particularly for system inventories and real-time risk exposure[6]. Preparing for insurance underwriting has become a team effort, requiring engagement from key stakeholders across the organization and comprehensive automated systems.

1 https://www.ajg.com/us/-/media/files/gallagher/us/2024/2024-cyber-insurance-market-conditions-outlook.pdf#page=7

2 https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2024.html

3 Ibid

4 https://woodruffsawyer.com/sites/default/files/document/Cyber%20Looking%20Ahead%20Guide%202024.pdf

5 https://www.reedsmith.com/en/perspectives/cyber-insurance-claims/2023/06/policyholders-seeking-cyber-coverage-face-increasing-underwriting-demands

6 https://riskandinsurance.com/u-s-cyber-insurance-market-to-harden-in-2024-survey/

Attack surfaces change daily. To address this continuous change, organizations require a continuous solution.

The complexity of modern organizations makes it difficult to collect this. Attack surfaces change daily, as organizations adopt faster development cycles, increasingly move to the cloud, and incorporate edge computing devices. To address this continuous change, organizations require a continuous solution.

Intro to CTEM

Continuous Threat Exposure Management (CTEM) is a security testing framework that identifies and mitigates cyber risks. CTEM emphasizes continuous testing and aligns testing efforts with core business objectives. Its ability to scale across complex attack surfaces and produce actionable outcomes has made it popular among large enterprises, and CTEM was recently placed at the top of Gartner's 2024 Security Operations Hype Cycle[7].

Gartner proposed a five-step cycle[8] to implement CTEM: Scoping, Discovery, Prioritization, Validation, and Mobilization. While organizations do not need to follow this structure verbatim, it is a useful starting description for a continuous program.

1. Scoping:
   Determine what the testing program is responsible for.
2. Discovery:
   Detect risks in scoped assets.
3. Prioritization:
   Order detected risks by impact to the organization
4. Validation:
   Determine which detected risks pose a genuine threat.
5. Mobilization:
   Address valid risks and improve higher-level security posture.

7 https://thehackernews.com/2024/08/ctem-in-spotlight-how-gartners-new.html

8 https://www.gartner.com/en/articles/how-to-manage-cybersecurity-threats-not-episodes

9 https://www.praetorian.com/resources/continuous-threat-exposure-management

For a comprehensive introduction to CTEM, we recommend "CTEM: A Modern Blueprint for Risk Prioritization and Reduction."[9]

We now discuss how each step of Gartner's CTEM cycle can help organizations navigate their insurance underwriting.

Scoping

Phase Objective: Determine the assets you will test.

During the Scoping phase, organizations map core business objectives to cyber asset classes (or individual assets, for smaller organizations). The organization then ranks the assets in order of criticality, factoring in both the criticality of the asset to its objective and of the objective to the business. Organizations may use quantitative risk analysis to numerically rank assets, or they can rely on qualitative metrics.

Because organizations must tie scoped assets back to business objectives, it's crucial to engage stakeholders across the business in this phase. By securing cross-organization buy-in early, the security team will have an easier time convincing their non-technical counterparts to implement initiatives later in the CTEM cycle.

With a ranked list of assets in hand, the organization then chooses the top subset they have resources to feasibly cover.

Relation to Underwriting

During the Scoping phase, organizations must prioritize assets that are crucial to business success. This will give organizations a better sense of what a compromise of each asset would mean for the business and how to allocate security resources. In turn, this understanding will make it clearer what an insurance claim might look like following a cyber event.

The Scoping phase also engages stakeholders across the organization, making them more involved in the security program. This first step gives those stakeholders a baseline context for the organization's cyber risks, making it easier to re-engage those stakeholders during the underwriting process as needed.

Discovery

Phase Objective: Map scoped asset classes to live systems and components.

In the Discovery phase, organizations scan systems in the scoped asset categories to create a comprehensive inventory of all individual assets, where those assets sit in the overall attack surface, what software runs on those assets, and what risks or vulnerabilities may be present in those assets. The result is a detailed database about the organization's attack surface, including a continuous list of vulnerability alerts to address.

Relation to Underwriting

The job of an underwriter is significantly easier if they have a detailed understanding of what they are insuring. Inadequate real-time cyber exposure data was ranked the top challenge in underwriting in a recent poll of cyber insurance underwriters[10]. Underwriters will be far more confident in an organization's ability to prevent cyber incidents if the organization has strong evidence of its ability to discover assets and detect risks in its digital landscape. In turn, this will result in an easier underwriting process and possibly a lower premium.

10 https://riskandinsurance.com/u-s-cyber-insurance-market-to-harden-in-2024-survey/

Prioritization

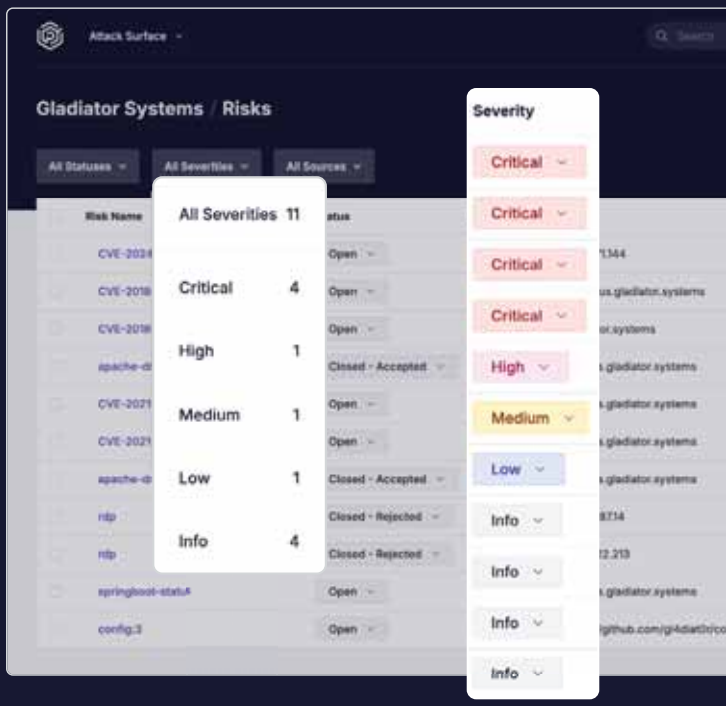
Phase Objective: Prioritize the vulnerability alerts by impact on the business.

In Prioritization, the organization uses a repeatable schema to estimate the risk of each detected alert to the overall business. The schema should be computer-friendly and should incorporate core business objectives. For example, an organization might devise numerical ratings to measure an asset's importance to business objectives, and then combine this measurement with the vulnerability's raw CVSS score, the number of impacted assets, and the age of the vulnerability into one score.

Using a computer-friendly schema allows automated solutions to perform much of the early grunt work in vulnerability triage. A properly tuned schema will cut out a significant chunk of false positive alerts, allowing manual reviewers to more time on higher-value tasks.

Relation to Underwriting

A comprehensive prioritization schema empowers organizations to efficiently allocate security resources. It is the first line of defense against wasted security analyst time, which will demonstrate a stronger ability to catch risks early. This schema also shows the underwriter the business has thought deeply about measuring risk and incorporated those conclusions into an actionable process.



Validation

Phase Objective: Determine the actual impact of detected vulnerabilities.

In the Validation phase, security analysts review each vulnerability alert to determine if it is exploitable, what the business impact is, and what mitigating controls may be in place. Validation allows security teams to further prioritize security alerts before contacting the necessary stakeholders for remediation.

1. Confirm if attackers can actually exploit the vulnerability
2. Determine what assets are at risk by exploiting the vulnerability
3. Investigate what compensating defensive controls exist and how they respond to a compromise

Relation to Underwriting

A well-defined Validation process is the start of a paper trail that measures an organization's ability to detect and remediate vulnerabilities. This phase will provide statistics on the number of vulnerabilities caught by the security program, the average criticality of a detected vulnerability, the average time to detect a vulnerability, and other information that will aid the underwriter's decision.

Mobilization

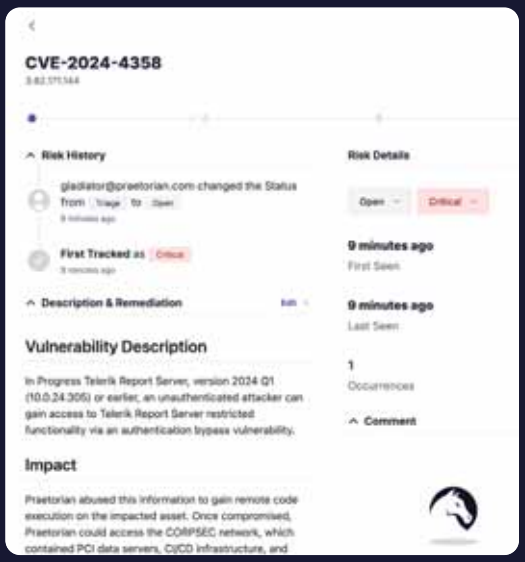
Phase Objective: Address all true positive alerts

After validating each vulnerability, the organization must determine what to do about it. During Mobilization, the security team contacts the associated asset's stakeholders to provide them with remediation steps. The security team may also collect data to inform higher-level security initiatives like changing/adding tools, enhancing authentication, or adding network-layer controls.

When implementing a CTEM program, the security team needs to engage their non-technical counterparts across the organization to determine how the organization will handle security alerts. This step creates a shared communication channel, making it easier to re-engage stakeholders later. Additionally, by tying vulnerability ratings back to business objectives, security teams will have an easier time convincing their coworkers of each initiative's importance.

Relation to Underwriting

The Mobilization phase demonstrates the organization's ability to effectively address security risks. It allows organizations to accurately collect statistics on the number of risks remediated, the average time of remediation, trends in risk frequency and type, and other useful information for the underwriter. Underwriters who see tangible proof of this will be more likely to approve insurance coverage or lower a premium.



Summary

CTEM is a security framework that emphasizes continuous testing and cross-organization engagement. This framework empowers organizations to collect a wealth of security and risk data about their cyber infrastructure, which will facilitate the cyber underwriting process.

CTEM with Chariot

Praetorian's Chariot platform is designed to embody the principles of CTEM, by combining people, process, and technology. Chariot incorporates attack surface management, vulnerability management, attack path mapping, breach and attack simulation, continuous penetration testing/red teaming, and exploit/threat intelligence into a single solution. These components, wrapped in a managed service, work in complete unison to provide unparalleled security coverage.

Contact Praetorian | Start Free Trial