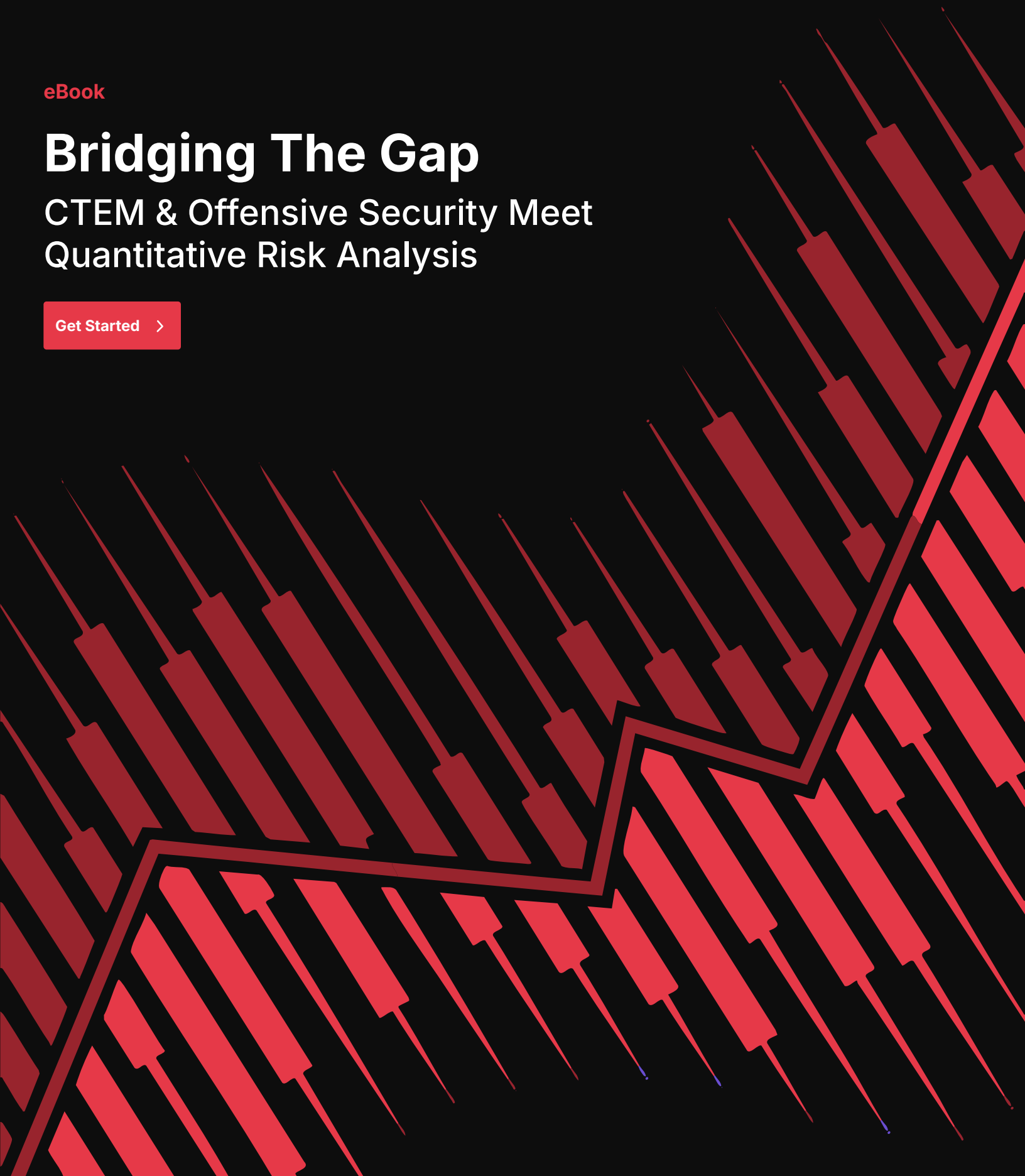
PRAETORIAN

eBook

Bridging The Gap

CTEM & Offensive Security Meet Quantitative Risk Analysis

Get Started >



Inside this eBook

Introduction

Many of our client organizations face the persistent challenge of quantifying cyber risk. Risk quantification is a messy but necessary task. It is difficult[1] to make business justifications for allocating resources toward security without a numerical means of measuring[2] the benefit the organization will receive. But cyber risks are generally qualitative and present no obvious solution for numerical representation.

Praetorian is creating a world free from security compromise. As such, we prioritize actionable recommendations over theory or opinion on the threats and vulnerabilities facing your organization. While frameworks like Factor Analysis of Information Risk (FAIR) offer structured approaches to risk quantification, they often rely on theoretical models and assumptions[3] that do not clearly connect with reality. If you've used FAIR or similar frameworks before, you might have ended the exercise thinking "Now what?"
This eBook aims to provide actionable advice for organizations looking to quantify their cyber risks. How do we bridge the gap between models like FAIR and an organization's real-world security posture?

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

Bridging The Gap

One great approach to this challenge is to incorporate data from offensive security activities into risk quantification models. Risk quantification is a data-driven challenge, and the more data your organization has on its security[4] landscape, the easier it will be to quantify risks. This necessitates a move toward a security testing framework that continuously generates data to provide organizations with real-time insight into their risk posture.

Continuous Threat Exposure Management (CTEM) is a rising security framework that uses continuous testing guided by business objectives to identify and mitigate security risks.

For readers unfamiliar with CTEM, we recommend reading our eBook, **Continuous Threat Exposure Management: A Modern Blueprint for Risk Prioritization and Reduction** before continuing.

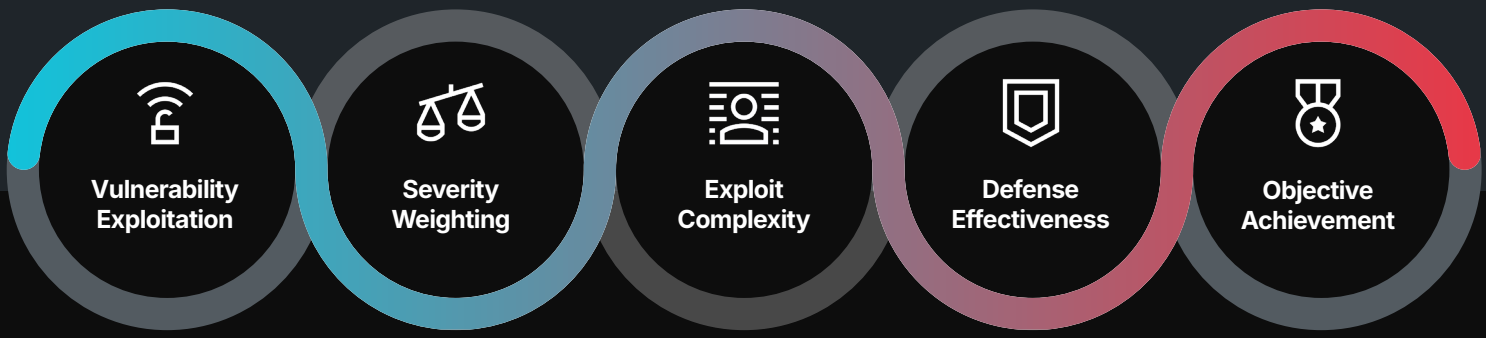
Because CTEM uses continuous testing, organizations gain real-time, data-driven insights into their security posture. This data can be directly incorporated into risk quantification models, providing empirical evidence to support or refine quantitative risk estimates

Let's dive into how we can use the output of a CTEM program to inform key components of quantitative risk analysis: Vulnerability (VULN), Threat Event Frequency (TEF), and Loss Magnitude (LM). In our examples, these values are intended to represent the respective median. In practice, it's also recommended to develop scenarios that demonstrate realistic minimum and maximum loss.

Refining Vulnerability Estimates

In FAIR, VULN represents the probability that a threat event will become a loss event. A threat event is an incident where a malicious actor successfully exploits a vulnerability or weakness in an organization's assets, systems, or processes. A loss event is a threat incident that results in material damage or harm.

Real threat and loss events are an excellent source of this data but are typically too infrequent to serve as a sound basis for calculations. Organizations can augment with data from simulated threats, including red teams, penetration tests, breach and attack simulations (BAS), and other CTEM exercises. Here's an example of how we can use CTEM exercises to determine a VULN score:



Vulnerability Exploitation

Use the number of vulnerabilities successfully exploited compared to the total number found. For example, if all CTEM exercises discovered 50 unique vulnerabilities and successfully exploited two, the initial VULN estimate could be 2/50 = 0.04.

Vulnerability Exploitation

Consider the severity of discovered vulnerabilities using CVSS or EPSS scores. For instance, for each discovered vulnerability carrying a CVSS score greater than 9.0 (Critical), you might apply

a modifier of +.005. Likewise, you might apply modifiers of +.003 for High (7.0 – 8.9), +.001 for Medium (4.0 – 6.9), and +.000 for Low (0.1 – 3.9). The specific modifier values are less important, so long as they allow you to factor the CVSS or EPSS score into the final vulnerability estimate and are consistent between calculations. For this example, we will assume the CTEM exercises discovered 1 high, 2 mediums, and 47 lows, resulting in a total modifier of +.005. This brings our current VULN estimate to 0.045.

Exploit Complexity

Organizations may also factor in the difficulty of exploiting each vulnerability. If one of the two exploited vulnerabilities required minimal skill, you might increase its respective modifier. As stated above, ranges are important. To determine a minimum and maximum of these values, you could tweak the complexity values to account for different types of attackers. An Advanced Persistent Threat (APT) may have an easier time exploiting something than a bored teenager, and thus the respective modifier score could increase further. For example, when modeling against an APT, we might double each exploited vulnerability's modifier. However, in this example, we skip this step and assume a uniform threat actor. Our VULN estimate remains at 0.045.

Defense Effectiveness

Assess how many security layers were bypassed during testing. Organizations should assign further modifiers for each type of security control in scope (EDRs, NDRs, 2FA, etc.) and increase VULN estimates based on the number of security controls the testers successfully bypassed. We will assume that in exploiting the two vulnerabilities, the testers successfully bypassed the affected workstations' EDR. We will also assume we assigned the EDR control a modifier of 0.005. This would bring the current VULN estimate to 0.05.

Objective Achievement

Consider how many key objectives a red team was able to achieve. Key security objectives should be tied to core business objectives (e.g., "unauthorized access to customer PCI data", or "unauthorized code deployment to production"). Similar to the above, each key objective should carry a further modifier to measure its impact. In this example, we will assume that neither of the exploited vulnerabilities allowed the testers to achieve a testing objective, which leaves the VULN estimate at 0.05.

Enhancing Threat Event Frequency (TEF) Estimates

TEF represents how often threat agents are likely to act against an asset. CTEM tools and exercises can provide insights you can use to determine:

Attack Frequency

Analyze how many distinct attack attempts were made during the engagement. For example, if a red team made 10 significant attempts over two weeks, this could extrapolate to 260 attempts per year.

Persistence Methods

Evaluate the techniques used to maintain access to systems. If the red team established two distinct persistent access methods, this might indicate more sophisticated, ongoing threat activity which warrants an increase in the TEF.

Attack Sophistication

Distinguish between simple probes and more complex attack attempts. If 10% of the attempts were considered "advanced", you might focus on these for your TEF calculation: 260 * 0.1 = 26 sophisticated attempts per year.

Temporal Patterns

Identify any time-based patterns in attack activity. For instance, if 60% of attacks occurred outside business hours, this could inform your defensive strategies and refine your TEF model.

Determining Attack Attempt

Attack frequency can be tricky since attack attempts are rarely evenly distributed. Perform the following to get a more accurate picture of attack attempt frequency:

Log Analysis

Review security logs, SIEM data, and IDS/IPS alerts. For example, if you observe 50 suspicious connection attempts per day, that's about 18,250 potential attacks per year. You could also take the average over the course of a few months and extrapolate that out to a year.

Honeypot Data

Deploy decoy systems to gather data on actual attack patterns. If a honeypot mimicking your SSO portal receives 5 attack attempts per day, that's about 1,825 annually.

Threat Intelligence

Use threat feeds to understand current attack trends in your industry. For instance, if reports indicate a 20% increase in attacks against CRM systems in the past year, you might adjust your frequency estimates accordingly.

Historical Data

Analyze your organization's past security incidents. If you've had 3 significant incidents in the past year, this provides a baseline for estimation.

Industry Benchmarks

Compare your data with peer organizations when possible. If similar-sized CRM companies in your region face an average of 1,000 significant attack attempts per year, use this to calibrate your estimates.

Estimating Loss Magnitude

Loss magnitude can be influenced by dozens of factors, which can be divided into “primary” and “secondary” losses. Primary losses are those immediately experienced during a loss event. Secondary losses have longer-lasting impacts after the loss event formally ends.

We’ve included some examples of both below:

Primary Losses

Productivity impact: 50 employees affected * $40/hour * 2 hours of downtime = $4,000

Incident response costs: 3 Incident Response staff * $60/hour * 10 hours = $1,800

System recovery expenses: $5,000 for emergency patches and updates

Data loss or corruption costs: 1,000 customer records * $150 per record = $150,000

Potential regulatory fines: $1,000,000 (2% of $50 million annual revenue per GDPR Article 83(4))

Total Primary Loss: $1,160,800

Secondary Losses

Reputational damage: 1% customer churn * 5,000 customers * $500 average customer value = $25,000

Legal expenses: $75,000 for potential lawsuits

Long-term market impact: 0.5% drop in annual revenue of $50 million = $250,000

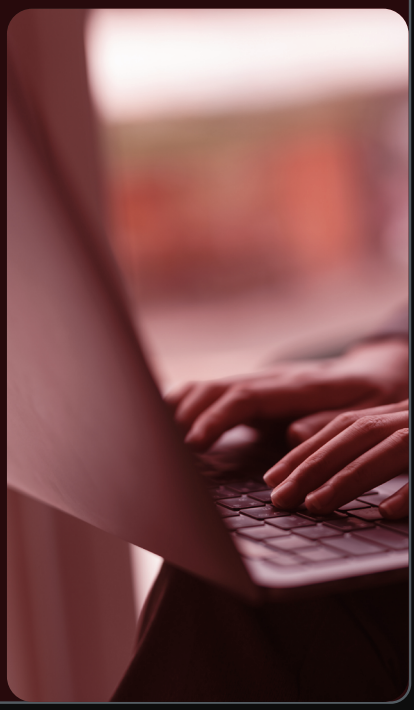
Total Secondary Loss: $350,000

Putting it into Practice: A Case Study

Let's consider a CRM software company that has developed its flagship product internally and has an annual revenue of $50 million. The company decides to conduct a FAIR analysis informed by recent CTEM exercises.

Key findings from the offensive security activities:

- ✓ 50 vulnerabilities discovered, 2 successfully exploited
- ✓ Red team achieved 1 out of 5 key objectives
- ✓ 10 significant attacks observed in a two-week period
- ✓ 10% of observed attacks were sophisticated enough to potentially succeed



Quantitative Risk Analysis inputs:

- ✓ Vulnerability (VULN): 0.05
- ✓ Threat Event Frequency (TEF): (10 * 26 weeks) = 260 threat events per year
- ✓ Loss Event Frequency (LEF) = TEF * Vuln = 260 * 0.05 = 1.3 loss events per year

Risk Calculation:

- ✓ Primary Risk: 1.30 * $1,160,800 = $1,509,040
- ✓ Secondary Risk: 1.30 * 0.3 * $350,000 = $136,500 (assuming 30% chance of secondary loss)
- ✓ Total Annualized Loss Expectancy (ALE): $1,509,040 + $136,500 = $1,645,540

Challenges in Adopting Risk Quantification

While this approach offers significant benefits, it's important to be aware of potential challenges:

Data Quality

The accuracy of your risk quantification heavily relies on the quality and relevance of data generated from your log and alerting systems. Poorly executed tests, too much noise from detection systems, or incomplete data can lead to misleading conclusions, which may undermine the reliability of your risk assessments.

Scope Alignment

Ensure that the scope of security tests aligns targets assets critical to core business objectives. Misalignment can result in overlooking critical vulnerabilities or overemphasizing less relevant ones, skewing the risk quantification process and potentially leading to inadequate or misdirected security measures.

Misalignment can result in overlooking critical vulnerabilities or overemphasizing less relevant ones

Evolving Threats

Regular updates are crucial as new vulnerabilities and attack techniques emerge. A continuous approach to scanning and testing is essential to keep pace with these changes and ensure your risk quantification remains relevant.

Estimation Bias

Human factors can introduce biases in estimating the ranges of probability and impact of potential security incidents.

Complexity

Balancing the level of detail required for accurate risk quantification with the need for usability and clarity can be challenging, particularly in complex systems involving multiple stakeholders or third-party integrations. The more complex the environment, the greater the difficulty in ensuring that the quantification remains both precise and actionable.

Benefits of this Approach

Data-Driven Decisions

By grounding your risk assessments in real-world data derived from security tests, you can move away from reliance on theoretical models or assumptions. This approach enables more informed and objective decision-making.

Improved Accuracy

Leveraging specific data points from CTEM tools and offensive security engagements provides a more accurate reflection of your actual security posture. This can help to pinpoint areas of weakness that might otherwise be overlooked, leading to a more precise and actionable risk profile.

Justified Investments

With concrete data supporting your risk assessments, you can more effectively justify security expenditures to stakeholders. This evidence-based approach helps ensure that investments are aligned with the actual risk, improving the overall efficiency and effectiveness of your security strategy.

Continuous Improvement

By creating a feedback loop between your security testing and risk assessment processes, you can foster an environment of continuous improvement. Regularly updating your risk models with new data helps to ensure that your organization remains resilient in the face of evolving threats.

Cross-Team Collaboration

This approach can foster close collaboration between your security and risk management teams. This partnership ensures that the data generated from security engagements is accurately interpreted and effectively utilized in the risk quantification process.

Conclusion

Integrating offensive security outputs into quantitative risk analysis creates a powerful, data-driven approach to cyber risk management. By grounding theoretical models in real-world testing data, organizations can develop a more accurate understanding of their risk exposure and make more informed decisions about security investments. A CTEM program further improves this practice by providing continuous coverage of the threats facing an organization.

In our case study, we saw how this approach led to a median annualized loss expectancy of $1,645,540 for a CRM company. This concrete figure, derived from the output of CTEM exercises, provides a clear justification for security investments and helps prioritize mitigation efforts.

While challenges exist in implementation, the benefits of this approach – including improved accuracy, actionable insights, and justified investments – make it a valuable tool for any organization seeking to enhance its cybersecurity posture.