FORTRA™

CISO's Guide to Justifying Offensive Security Investments

The role of Chief Information Security Officer (CISO) has evolved beyond IT and security to encompass strategic insight at the highest levels. Deloitte notes that a third of organizations have seen increased involvement from CISOs in strategic technology investment conversations, and there's every reason to believe that trend will continue. **As CISOs form security strategies in view of today's threat landscape, one thing is clear: a well-rounded approach that includes defensive and offensive tactics is the only viable option.**

That said, it's not uncommon for other stakeholders in an organization to require a little convincing. Budget conversations can be challenging, so it's important to be armed with the right value propositions when proposing spend on offensive security tactics like red teaming and penetration testing.

This guide will help CISOs—and others advocating for offensive security tactics—understand how to present these points effectively, connect them to key business objectives, and position offensive security as the strategic investment it has become.

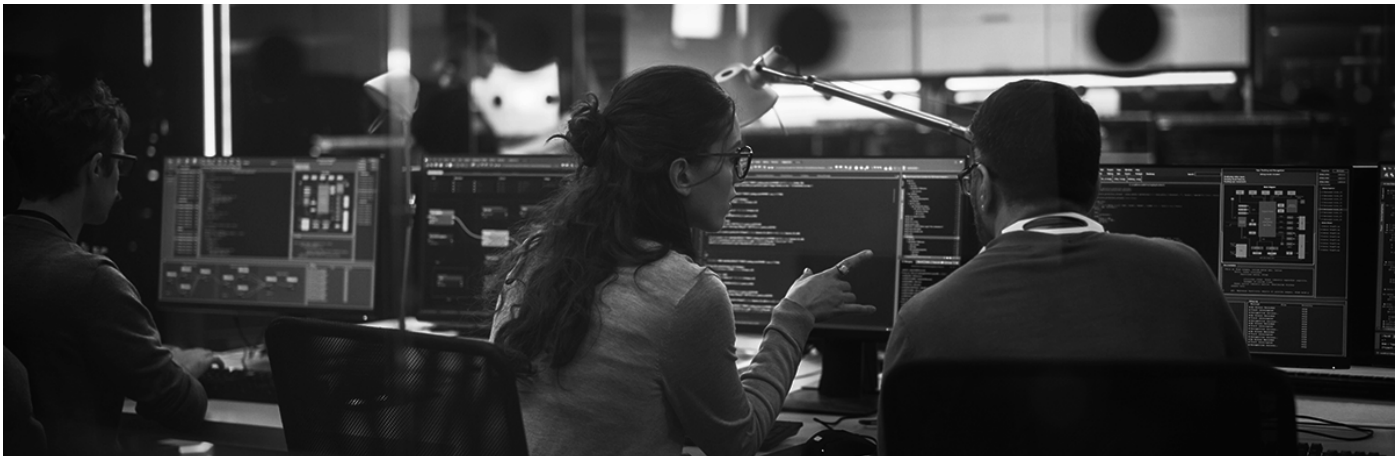


Table of Contents

The Compelling Case for Offensive Security

Offensive tactics drive resilience and readiness. In today's threat landscape, attackers gain new advantages daily with emerging technology and evolving methods to compromise systems. Without upgrading to offensive security techniques that reveal what attackers see and put their defenses to the test, organizations remain vulnerable to costly surprises.

Addressing Limitations of a Defense-only Security Strategy

The cybersecurity market is saturated with defensive security tools— firewalls, data classification, data loss prevention, email security, XDR, and more. Attackers know this and are becoming adept at getting around them.

As tools improve at catching signature-based threats, cybercriminals continue to craft malware that evades detection. AI now enables the rapid creation of polymorphic malware and other evasive techniques. It also allows hackers to automatically discover network vulnerabilities at unprecedented speeds and enhance advanced persistent threats (APTs) by accelerating learning, finding default credentials faster, and maintaining stealth.

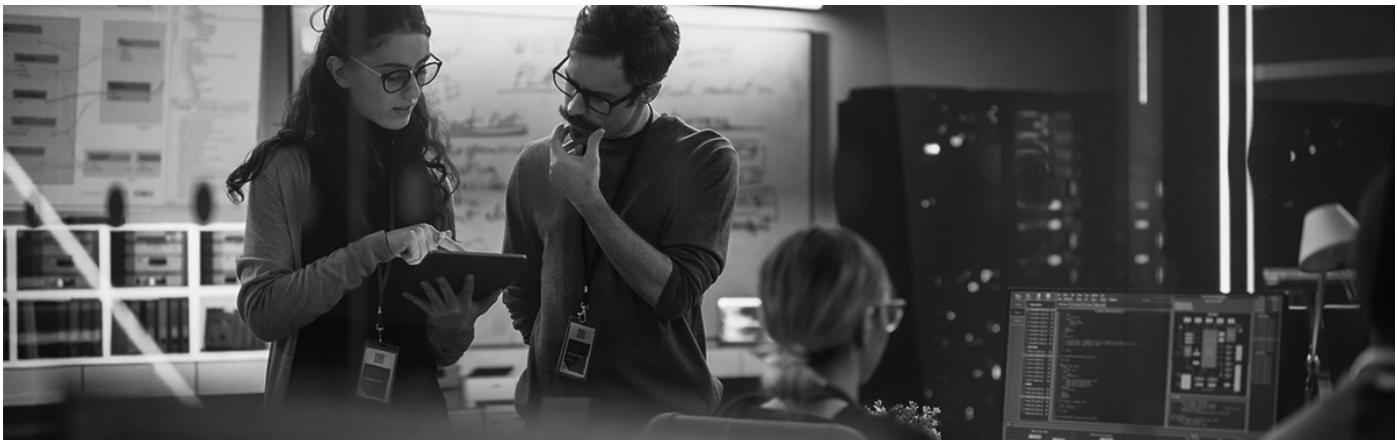
If organizations are being matched by technology on the defensive front, they need to adapt by engaging attackers earlier in the attack chain. With offensive security measures like pen testing tools and red teaming, security teams don't have to guess where threat actors might strike–they can know, because their defenses have already been battle tested through realistic attack simulations.

To keep your business out of the breach headlines, avoid compliance fines, and maintain consumer trust, you must proactively put your security controls and defenses to the test – because attackers surely will.

Mapping Offensive Tactics to Business Objectives

The C-suite must understand that offensive security directly supports essential bottom-line goals and KPIs. Given the rapid evolution of technology and the danger of detecting attacks too late, offensive security is emerging as the industry-standard method for ensuring data protection and compliance measures are effective.

- **Continuity, Growth, and Shareholder Value:** Nothing hinders growth more than reputational damage from a cyberattack, operational downtime incurred by a breach, or the loss of sales. Offensive security allows organizations to identify weak spots before attackers do, rather than waiting to be surprised. This increases the ability to guarantee uninterrupted growth and protected shareholder value.
- **Risk Management:** One of the core components of a CISO's role is to mitigate and manage risk at the highest level. While strong defensive security is necessary, it is no longer sufficient. It's like providing an army with weapons, but not additional intelligence on the enemy or on weaknesses in national defense. Penetration testing demonstrates potential attack paths, while red teaming shows your team where an advanced adversary can outmaneuver controls and defenses. The insights gained from these tests can:
  - Reduce mean time to detection (MTTD) and response (MTTR)
  - Accelerate time-to-remediation for high-risk weaknesses
  - Improve cyber insurance posture
  - Streamline and maintain compliance efforts



- **Competitive Advantage:** Cybersecurity is increasingly seen as a core competitive. As Forbes notes, "Investors and stakeholders increasingly recognize the importance of security, making it a fundamental consideration in their decision-making processes." Strong defensive and offensive security postures demonstrate to investors and markets that you are committed to long-term success, understand the relevance of cybersecurity modern business, and maintain a culture that goes beyond the "bare minimum" to truly protect key assets.
- **Compliance Requirements:** As offensive security techniques continue to prove their value against modern attacks, they are increasingly included in data privacy and security standards. Key compliance frameworks now explicitly require or strongly encourage offensive security measures:
  - **PCI DSS:** Organizations handling payment card data must perform penetration tests at least annually, or after making any significant changes to the environment.
  - **GDPR**: Article 32 requires data controllers and processors to regularly evaluate the effectiveness of their security measures, which penetration testing and red teaming directly facilitate.
  - **HIPAA:** HIPAA requires covered entities to conduct security risk analyses regularly, and the Security Rule's Evaluation Standard highlights the need for periodical technical evaluations. In December 2024, the US Department of Health and Human Services proposed updating the Rule to explicitly mandate annual pen testing and biannual vulnerability scanning.
  - **SOC2:** Auditors highly recommend penetration testing to satisfy specific Trust Services Criteria (TSC) to monitor activities and identify security weaknesses.
  - **ISO/IEC 27001:** Annex A emphasizes the need to not only find and mitigate vulnerabilities, but test security functionality – something facilitated by vulnerability management, pen testing, and red teaming.
  - **NIST CSF:** The "Identify" pillar of the NIST Cybersecurity Framework (CSF) states that organizations need to understand and discover weaknesses within their systems and controls. Offensive security techniques naturally lend themselves to this step.

Even where not directly mandated, offensive security controls are encouraged and even implied in leading compliance standards, representing the most effective approach to accomplishing required risk management. And, as is the case with HIPAA's new rule proposal, the trend is towards making these "suggestions" permanent.

ROI: Cost, Risk Reduction & Resilience

The Price of Inaction

The average data breach costs $4.88 million, according to IBM's Cost of an Average Data Breach Report 2024. While costs are lower for small businesses, the monetary size is relative and can be equally or more devastating. Compounding this, **93% of companies of all sizes that experienced prolonged data loss (over ten days) will file for bankruptcy within a year**. Well-known companies that ceased operations following a cyberattack include Travelex, DigiNotar, YouBit cryptocurrency exchange, and Code Spaces.

Additionally, attacks involving exploiting vulnerabilities as the initial attack vector rose by 34% year over year, bringing the total up to one in every five according to the Verizon 2025 Data Breach Investigations Report. Aside from that, some of the biggest cybersecurity incidents to shake the corporate world have been the direct result of exploitable network vulnerabilities: SolarWinds, Equifax, Yahoo, Mariott International, Uber, CapitalOne, and more.

The Investment Comparison

Comparatively, the cost of investing in offensive security through penetration testing, red teaming, and related tools is cost effective. These methods can reduce wasted resources by using an attacker mindset to identify genuinely exploitable weaknesses, allowing security teams to focus on closing the most critical gaps rather than addressing an unprioritized list of CVEs that may never be exploited.

Risk Reduction

Offensive security tools provide unmatched risk reduction as nothing establishes risk as well as proactive probes into the network, its apps, and the defensive measures set up to protect them.

Pen testing and red teaming can uncover:

- Shadow IT – Shadow APIs, Shadow Data, Shadow AI
- CVEs
- Scripting errors and coding flaws
- Misconfigurations
- Weak security controls
- Excessive permissions
- Holes in Identity and Access Management (IAM)
- Gaps in employee security awareness
- A propensity to click on phishing emails
- Faulty firewalls
- Detection and response workflow errors
- Weak points in supply chain security

Offensive security is one of the only truly responsible ways to assess and ultimately reduce risk, because it confirms whether weaknesses are exploitable and what level of damage a malicious actor could do if they infiltrate.

Building Resilience

Offensive Security measures identify exploitable weaknesses, allowing security teams to focus on closing the most critical gaps rather than addressing an unprioritized list of CVEs that may never be exploited. It is unwise for any organization with the power to gain more insight into viable attacker tactics to leave this intelligence on the table.

As summed up by the World Economic Forum in their Unpacking Cyber Resilience report, "Large-scale data breaches and supply-chain attacks, and the widespread adoption of emerging technologies leads to the rise of cyber resilience as a business enabler."

Getting Buy-In

Understanding the validity of an offensive security posture is the first step. The next challenge is successfully presenting these assertions in the boardroom and securing buy-in. Here are strategies for shaping your presentation:

- **Tell the Story:** Be selective with graphs, metrics, and statistics. Focus on the business narrative and save in-depth cybersecurity presentations for technical audiences. If the "story" doesn't emphasize bigger business objectives like compliance, resilience, competitive edge, risk reduction, and growth enablement, your C-suite audience won't engage.
- **Provide Perspective:** Help board members see beyond immediate costs. Resources will be spent either way—the question is how and at what ultimate cost. Avoiding a slight budget increase in offensive security now could mean doling out a huge investment in operational costs, PR coverups, getting data back online, making possible ransomware payouts, paying compliance fees, and doing all the cleanup that comes after a breach.
- **Communicate Risk:** Position offensive security techniques not as "nice extras" but as essential mitigation strategies that address already high-risk levels. Consider the sophistication and tenacity of today's threat actors and then consider the result of sticking your head in the sand and just assuming the defenses you have in place are enough.

Overcoming Internal Objections

Even with a strong case, expect pushback. Investing in a complete cybersecurity strategy that includes defensive *and* offensive security is a newer concept and rifts in the status quo are not always welcomed.
Here's how to overcome the inevitable internal objections to an offensive security plan:

1. **"We don't have the money."** Focus on ultimate value and long-term thinking. If too much budget goes to R&D, for example, how valuable are those findings if they can be stolen and sold? Without solid cyber protections, other investments lose their value.
2. **"We don't have the time or resources."** Again, first couch the problem in the fact that you don't have the money to gamble on a security breach that could put you under. Then add to that the fact that the right pen testing and red teaming tools will make your teams more efficient and effective, ultimately saving resources. And if you do not have pen testers and red teamers on staff, outsourcing to a third-party provider is an option that can help.
3. **"We are sufficiently protected without additional testing."** Don't let attackers do the testing for you, as their fees are far higher. Offensive security is not a matter of over-examining an already safe environment. It is built on the reality that the "human factor" is still present in 60% of breaches, per the Verizon 2025 DBIR. That means that even the best-laid security plans are still subject to oversight, misconfiguration, scripting errors, and a myriad of other entry points only attackers can find. Unless your organization takes the initiative and finds them first.

Step-by-Step Investment Roadmap

The ultimate goal is to have a healthy, thriving offensive security suite with end-to-end protection; from discovering vulnerabilities to facilitating advanced purple team engagements. However, to make changes lasting, they are going to have to be implemented step-by-step. This investment roadmap lays out what the process can look like for organizations looking to begin where they are.

- **Step 1: Assess Current State and Identify Offensive Security Needs.** Inventory existing capabilities. Do you have a pen testing team? Are third-party pen tests scheduled? Identify current activities and gaps relative to compliance requirements and risk intelligence needs.
- **Step 2: Establish Baseline with a Vulnerability Scan.** As Fortra's Mieng Lim, VP of Product Management, states, "[H]ow can you know where you're going without a roadmap? Your whole security setup is ostensibly to protect your internal assets from outside attackers. Great. Do you know where they're going to attack? If you had an accurate inventory of all your weak spots, you'd have a pretty good guess."
- **Step 3: Immediately Pair Scan Results with Pen Testing.** A vulnerability scan will put any penetration test ahead of the game. Instead of having to find vulnerabilities from scratch, the results of the scan will tell pen testers where to look, what to test, and what to exploit. As Lim sums up, "VM can tell you how many vulns you have and where they reside, while pen testing identifies which of those CVEs presents the greatest potential for compromise."
- **Step 4: Remediate and Validate with Additional Testing.** After applying patches to the most important vulnerabilities (the right VM program will automatically prioritize these for you based on severity), it's time to see what else a motivated attacker can do. While pen testing operates within a defined scope and checks regulatory boxes, red teaming tests your organization's entire defensive capabilities, assessing deficiencies in not only controls but in overall response (from alerts to SOC actions) and provides an outbrief of what could have (and should have) been caught so security teams know exactly where attackers can get in. Fortra's Core Impact provides pen testing software and works with Cobalt Strike and Outflank Security Tooling (OST), de facto standards for red teaming tools. Using these tools together enables teams to perform advanced red team engagements with relative ease.
- **Step 5: Implement Purple Team Collaboration.** Purple teaming means that both offensive and defensive security groups share information with the intent to inform the company of overall weaknesses – rather than on "winning" and keeping "trade secrets" to themselves. This is one of the investments (be it in-house or paired with an MSSP) that will help organizations see the greatest ROI from their red team technology investment.

Conclusion

Attackers are overwhelming defensive cybersecurity measures, and without a full offensive/defensive arsenal, organizations today are sitting ducks to advanced and emerging attacks.

A complex digital landscape and even more complex workplace challenges have led to distributed services, environments, and security resources. A lot can fall through the cracks, and without proactive offensive security measures to make sure things are working as intended, companies can be at risk and not even know it.

These factors create unnaturally high risk levels across organizations of all sizes, exacerbated by limited enemy knowledge and incomplete attack surface understanding. As CISOs effectively communicate these realities, offensive security will be recognized for what it is—the essential approach to eliminating security blind spots and meeting attackers on equal footing.

Appendices

Glossary

- **Defensive Security**: Defensive security encompasses safeguarding data, files, employees, your brand reputation, and the network through solutions like data security posture management (DSPM), cloud access security broker (CASB), data loss prevention (DLP), data classification, integrity and compliance monitoring, human risk management, vulnerability management, email security, extended detection and response (XDR), and brand protection.
- **Offensive Security:** Offensive security emulates the tactics, techniques, and procedures (TTPs) of an adversary to provide the organization with in-depth information about system and network weaknesses not readily attainable in any other way – besides a malicious attack. These solutions include penetration testing and red teaming.
- **Vulnerability Management:** Vulnerability management identifies, evaluates, reports, and prioritizes vulnerabilities (system weaknesses) within the network so that organizations can patch them and prevent easy exploitation by attackers.
- **Penetration Testing:** Penetration testing focuses on finding and exploiting vulnerabilities within a predefined area of the network, often using the results of a previous vulnerability scan as a head start.
- **Red Teaming:** Red teaming simulates a real-world attack by advanced threat actors, broadening the scope to include a wider area of the network (if not the whole thing), and testing the overall detection and response capabilities of an organization – from solutions to SOCs. This video explains When to Use Pen Testing, Red Teaming, or Both.
- **Purple Teaming**: Purple teaming is a mindset that facilitates more effective offensive security engagements. A purple team is a collaborative group, or group mentality, that combines both red and blue team thinking to improve the overall security posture of an organization.

Proposals to Require Risk Management Accountability

The Securities and Exchange Commission (SEC) is proposing to require organizations to explicitly detail their policies and procedures for risk management, if any. See the SEC's Final Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure.

"The Commission proposed to add 17 CFR 229.106(b) (Regulation S-K "Item 106(b)") to require registrants to provide more consistent and informative disclosure regarding their cybersecurity risk management and strategy in their annual reports…

Proposed Item 106(b) would require a description of the registrant's policies and procedures, if any, for the identification and management of cybersecurity threats, including, but not limited to: operational risk (i.e., disruption of business operations); intellectual property theft; fraud; extortion; harm to employees or customers; violation of privacy laws and other litigation and legal risk; and reputational risk."

This includes, among other things:

- "Whether the registrant has a cybersecurity risk assessment program and if so, a description of the program."
- "Whether the registrant undertakes activities to prevent, detect, and minimize effects of cybersecurity incidents."
- "Whether cybersecurity risks are considered as part of the registrant's business strategy, financial planning, and capital allocation and if so, how."

Offensive Security Maturity Checklist

Seeing the vision and gaining decision-maker buy-in is step one to completing your security strategy with offensive security. Step two is to give your organization the greatest chance of success. This Offensive Security Maturity Checklist will help you gauge when your team is overdue for the next step:

1. **Are you anticipating an audit?** Regulatory requirements are the first green flag for offensive security techniques. Standards like PCI DSS, GDPR, NIS2, HIPAA and more either mandate or strongly encourage risk assessment via vulnerability management, pen testing, and red team engagements.
2. **Have you had a recent security breach?** Two-thirds of those hit by cyberattacks are targeted for attack again. A data breach is the perfect opportunity to dive in with a team of white hats and see what attackers see – and secure it before another attack.
3. **Have you merged, acquired, or made recent system changes – including cloud migration?** The chances of error during periods of volatility are high. Security mistakes like misconfigurations, oversights, Shadow IT, and more can be especially common during technical transitions. Offensive security testing can make sure everything was deployed correctly and that no security gaps threaten the organization at an already vulnerable time.
4. **Have you assessed third-party risk?** As host companies are increasingly being required to assume full responsibility for third-party threats, offensive security testing can provide two distinct benefits. First, it can ensure that your company is aware of security gaps in onboarding (access management issues, excessive permissions). Secondly, if applied to your third parties, offensive security testing can reveal hidden external weaknesses of which your company should be aware.
5. **Does your business have a strong defensive security posture in place?** The goal of offensive security is to test mature security postures at their best. If there are core components of your defensive security posture missing, like DLP, data classification, email security, or automated detection and response, it may be good to fill those holes before moving forward. How few or how many solutions is up to you; the point is to test the solutions, workflows, and processes your organization plans on having in play at the time of an attack.

FORTRA™

Fortra.com

About Fortra

Fortra provides advanced offensive and defensive security solutions that deliver comprehensive protection across the cyber kill chain. With complete visibility across the attack chain, access to threat intelligence spanning the globe, and flexible solution delivery, Fortra customers can anticipate criminal behavior and strengthen their defenses in real time. Break the chain at fortra.com.

(fta-gd-0825-r1-gm)