Cobalt

THE OFFSEC SHIFT REPORT

Secure tomorrow, today.

A COBALT PUBLICATION

INTRODUCTION

When people think of cybersecurity, most only think of defensive measures. After all, one of the most common images associated with cybersecurity is a shield. And this makes sense - cybersecurity measures have long stood as the line of defense against costly attacks.

But is a defensive strategy enough on its own? What would happen if we brought offensive measures into the mix - a sword to accompany our shield? An integrated strategy provides invaluable data about potential weak points in an organization's resilience and helps identify the best way to remediate them.

"OFFSEC DEFINED"

Offensive cybersecurity preemptively identifies vulnerabilities and security weaknesses before an attacker exploits them. Offensive cybersecurity teams - AKA "red teams" - actively test the network's defenses and provide meaningful insights into an organization's cybersecurity posture.

To understand the evolving state of cybersecurity risks and the shift towards blending defensive and offensive strategies, Cobalt recently surveyed more than 1,200 security professionals working full-time in the United States and United Kingdom across the following roles:

- DevOps
- SecOps
- IT Security
- Network Security
- Cloud Security
- InfoSec

The OffSec Shift Report reveals how organizations are adapting to bring both defensive and offensive strategies to the cybersecurity battle. Let's explore what respondents shared about the evolving threat landscape, how they're evaluating a shift in approach, and how you can apply these learnings to your organization.

THE COST DYNAMICS OF CYBERSECURITY

The past year was hard on cybersecurity teams.. The persistent economic downturn led to 39% of organizations deprioritizing their cybersecurity strategy. ***Note: those working in retail/consumer products were 46% more likely than average to say this.***

As such, organizations are facing an uphill battle when safeguarding their digital assets. Forty-one percent noted they don't feel confident that their company's current defensive cybersecurity measures are effective - an endeavor that currently utilizes an average of 38% of total security budgets. Those who decreased budgets in the last 12 months are especially likely to feel wary here: these respondents were 81% more likely than average to lack confidence in the effectiveness of their company's defensive cybersecurity measures.

While 54% of companies increased their security budgets in 2023, those funds were primarily used to maintain the status quo rather than innovate. In fact, more than half (55%) of respondents shared that due to tight budgets, their team pivoted from expanding new investments in order to focus on optimizing existing resources. Let's explore where that money went.

Inside the cybersecurity budget

The financial implications of cybersecurity are twofold. One side of the coin, so to speak, involves investments in efforts and tech tools to improve companies' overall security posture. Time is money, and both DevOps and SecOps professionals spend a significant amount of time managing their security tools:

Average time managing their tools

28

Average hours **SecOps** spends per week

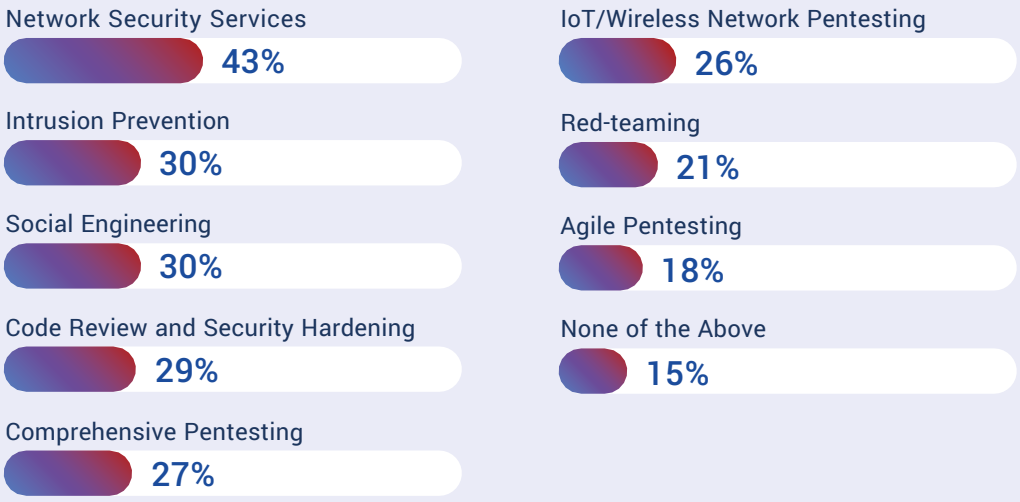
22

Average hours **DevOps** spends per week

Note: SecOps professionals in the U.S. spend 11 more hours on average managing security tools each week than their U.K. counterparts.

This time suck leads many teams to outsource such responsibilities. Companies are currently outsourcing the following offensive security strategies through a third-party or technical provider:

Services outscourced by security teams



Most (93%) of those who outsource pentesting say PtaaS is responsible for their proactive stance in identifying and mitigating potential security vulnerabilities. Those who outsource agile pentesting also reported that it saves them an average of 23 hours per week addressing potential vulnerabilities, enhancing their overall security posture by an average of 31%.

COMPARISON: U.S. VS. U.K.

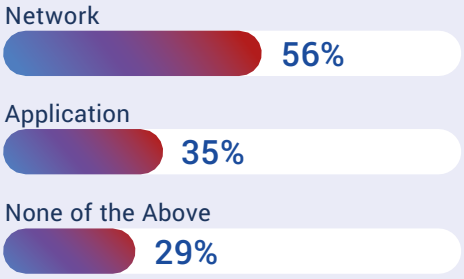
U.K.-based respondents are seeing reduced security investments at a higher rate: these respondents were 50% more likely than those in the U.S. to say their security budget has actually decreased in the past 12 months.

We also found that U.S.-based companies, despite being marginally less likely to outsource agile pentesting, showcase superior time savings and ROI. For those that outsource agile pentesting in the U.S., this manifests in average weekly time savings of over 26 hours and 34% increase in overall security posture, contrasting with 20 hours and 28%, respectively, reported by their U.K. counterparts.

The other side of the coin involves the ever-growing cost of data breaches. The financial impact of cyber attacks is terrifyingly high, and it's only continuing to grow: three in four respondents reported that the financial impact of data breaches has increased in the last year, amounting to massive losses for companies. Panelists estimated that 23% of security breaches are successful per year, each costing companies an average of $1.6M.

Consider vulnerability exploits as an example. Such incidents often lead to cybersecurity breaches, with network exploits emerging as the most common target. Of those who have experienced exploits in the past year, 51% noted that at least one in four of these resulted in major data breaches.

Which of the following vulnerability exploits have led to incidents in the last 12 months?



However, threat level and budget are often misaligned. Respondents who reported their company prioritizes continuous testing of the entire attack surface noted that only 25% of their budget is allocated towards safeguarding network vulnerabilities, and only 24% is allocated towards applications.

COMPARISON: U.S. VS. U.K.

While both markets experienced vulnerability exploits in 2023, U.K.-based companies were more likely to avoid major data breaches. These respondents were 20% more likely than their U.S. counterparts to report that less than 25% of the exploits they experienced in the past year resulted in significant breaches.

UNLEASH THE POWER OF ADAPTIVE RESILIENCE

As breaches become more costly, the majority of organizations are stepping up their offensive security measures. One key method for doing so is pentesting: 75% of respondents told us their company conducted more regular pentesting in 2023 than 2022. The results? Speeding up their team's incident response times (86%) and decreasing successful breaches by over 50% (82% of respondents saw this result in the past 12 months).

A holistic approach

Another major consideration for cybersecurity leaders is the split between blue team and red team operations. Unlocking cyber resilience means finding the sweet spot between offensive and defensive measures. Let's dive into how this split is currently playing out.

BLUE VS. RED TEAMS

Blue teams are responsible for defensive measures, like monitoring, detecting, and responding to security threats in real time. Red teams, on the other hand, employ offensive tactics to test their organization's security defenses. The most effective approach to cybersecurity will be a blend between the two (also known as "purple-teaming").

Nearly half of all respondents to the OffSec Shift Report (47%) told us they increased investments in blue team operations in 2023. Budget allocations primarily targeted digital risk protection (59%), attack surface monitoring (47%), and breach attack simulations (46%). Note: U.S.-based companies that increased blue team investments were 19% more likely than their U.K.-based counterparts to invest in breach attack simulations.

The returns were overall positive: an overwhelming majority of those who increased blue team investments (95%) noted that it optimized their team's response times, while 88% reported it allowed their teams to effectively mitigate security incidents.

Meanwhile, organizations are using red team exercises to shed light on potential vulnerabilities. Sixty-three percent of respondents agreed they conduct more red team exercises now than they did last year. Of those, 81% said this decreased successful breaches by over 50% in the last 12 months, and 85% reported these measures significantly sped up their team's incident response times.

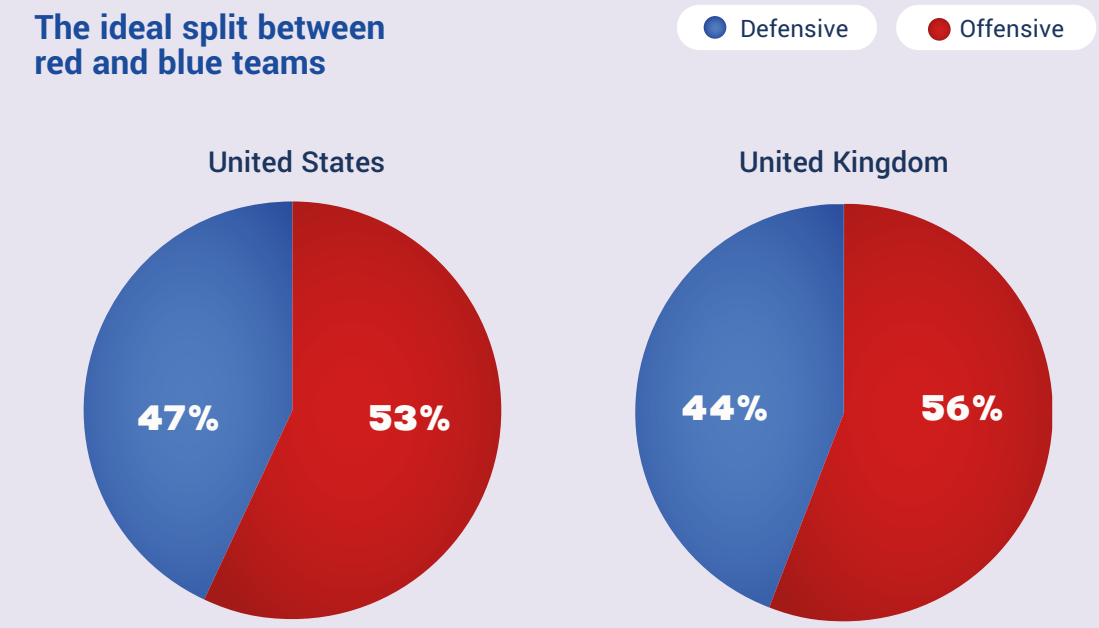
This proven efficacy is leading many to advocate for a boost to OffSec investments, with nearly three in four (74%) agreeing their company's cybersecurity would be stronger if more budget were allocated towards OffSec measures. And with 84% of those who increased blue team investments planning to do the same for OffSec in the next year, it's evident that a shift towards offensive, adaptive resilience is on the horizon.

Finding the ideal split between offense and defense

Many organizations are already embracing a holistic approach. Sixty-two percent told us their company currently implements joint blue-red team exercises to foster collaboration, and another 77% prioritize continuous security testing of their entire attack surface.

As for the ideal split between red and blue, here's what respondents had to say:

The ideal split between red and blue teams



So-called "purple-team" operations are on the rise, with more than a third of organizations increasing investments in such measures over the past year. And they're already seeing high returns: 93% of those who have expanded investments here say blue-red integration has enhanced their company's cybersecurity capabilities.

ELEVATING CYBERSECURITY TO A BOARD-LEVEL CONVERSATION

Organizational resilience is deeply intertwined with executive strategy. Without buy-in from the highest levels of leadership, prioritizing company-wide cybersecurity becomes a losing battle. Investment in critical tools and initiatives can become more difficult to secure. Organizations can underestimate the threat landscape or overestimate their risk tolerance.

Organizational resilience is deeply intertwined with executive strategy. Without buy-in from the highest levels of leadership, prioritizing company-wide cybersecurity becomes a losing battle. Investment in critical tools and initiatives can become more difficult to secure. Organizations can underestimate the threat landscape or overestimate their risk tolerance.

But there's a disparity between the value we place on executives' role here and how this actually plays out. While 89% of respondents said they believe C-level involvement is critical to a successful security posture, 35% told us their organization lacks a C-level-focused security strategy.

When executives aren't invested, it leaves SecOps and DevOps professionals worried: those without C-level-focused strategies were 27% more likely than others to lack confidence in the effectiveness of their company's current defensive measures.

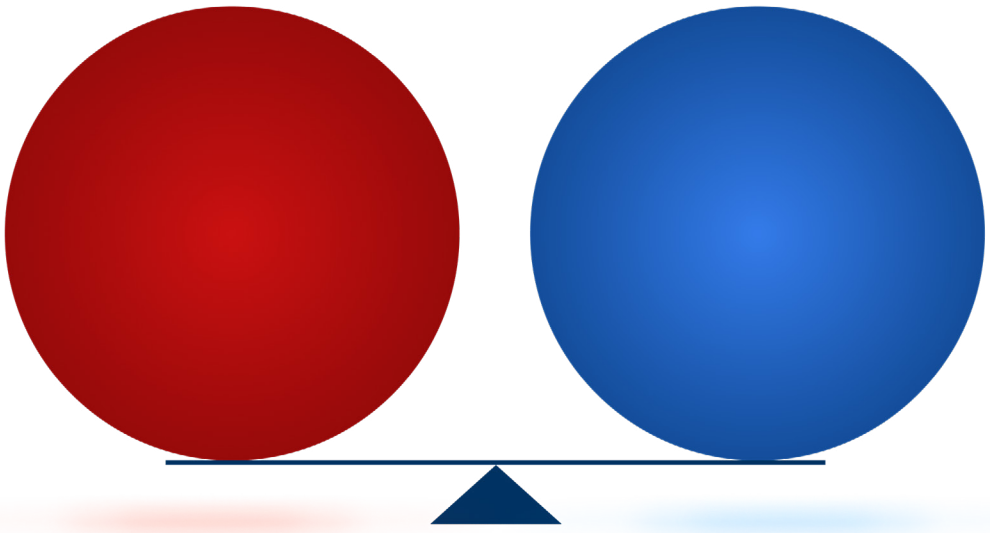
Conversely, companies with higher levels of C-Suite involvement experience a cybersecurity surge. Those with C-level-focused strategies didn't stall on innovation - in fact, they were more likely to have increased pentesting (41%) and purple team investments in the last year (72%). These respondents were also 80% more likely to say their company has increased its security budget in the last 12 months. This highlights that C-level involvement is the key to unlocking the next level of cyber resilience.organizations can operate fearlessly and innovate securely.

CONCLUSION

While the OffSec shift is certainly underway, there's still a long way to go: 58% of respondents believe their company is still lagging in integrating OffSec practices into their security strategies.

Organizations looking to strengthen their overall security posture in 2024 and beyond must work to obtain C-level buy-in on cybersecurity initiatives and identify and execute the ideal split between blue and red team operations. This will help illuminate budgetary priorities when it comes to outsourcing, tech spending, and manpower.

Investing in comprehensive security solutions is an absolute necessity for ensuring resilience and protecting digital assets in today's ever-evolving threat landscape.



For guidance on striking the perfect balance between defensive and offensive measures, **connect with Cobalt today!**

About Cobalt

Cobalt infuses manual pentesting with speed, simplicity, and transparency. Our award-winning Pentest as a Service (PtaaS) model empowers organizations to keep pace with their evolving attack surface and agile software development lifecycles. Thousands of customers and hundreds of partners rely on Cobalt's modern SaaS platform and exclusive community of more than 400 trusted security experts to secure applications, networks, and devices. We deliver pentests that support business drivers, maximize internal resources, and create stronger security programs so that organizations can operate fearlessly and innovate securely.

Survey methodology and demographics

The OffSec Shift Report survey was conducted between January 8 and January 23, 2024. Cobalt surveyed a total of 1,255 respondents in the United States and the United Kingdom who are employed full-time in a DevOps or SecOps, IT Security, Network Security, Cloud Security, or InfoSec role. The study was conducted at 95% confidence with a +/- 4% margin of error.

Cobalt

COBALT.IO