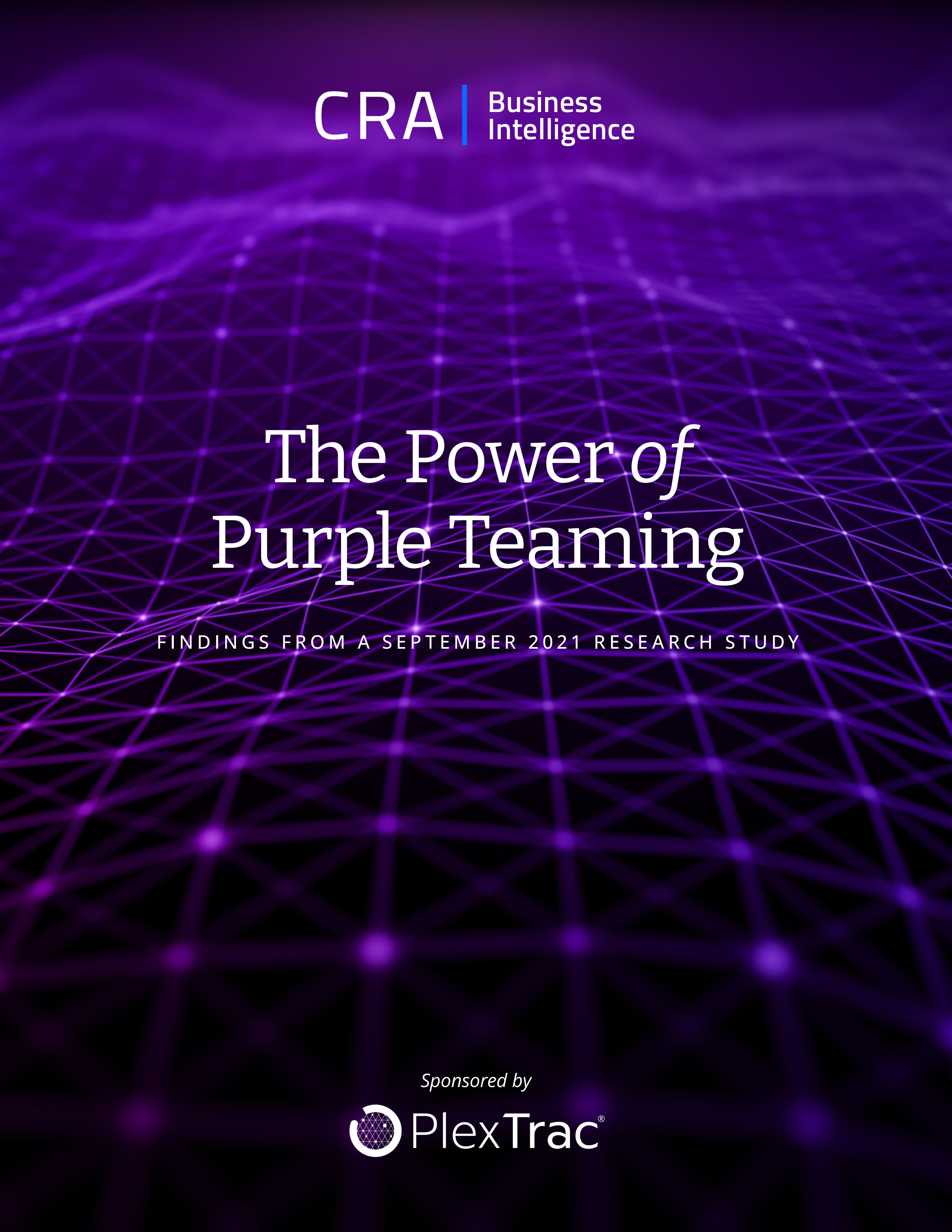


CRA | Business Intelligence

The Power *of* Purple Teaming

FINDINGS FROM A SEPTEMBER 2021 RESEARCH STUDY

Sponsored by

PlexTrac®

1

The Power *of* Purple Teaming

BACKGROUND

As the threat landscape evolves and cyber risks expand, enterprises are always looking to stay ahead of adversaries who wish to do harm. Whether it’s to prevent a ransomware attack or stymy some other advanced threat, organizations benefit from coordinated exercises that periodically test the hardiness of current tactics, techniques, and technologies to see what shakes out. One widely acknowledged approach is establishing teams of penetration testers to find and remediate vulnerabilities and gauge incident response plans. Increasingly, these intentionally antagonistic programs are shifting from a purely competitive model to a more collaborative one — where these teams play alongside, rather than against, each other.

That approach is known as purple teaming — pre-planned exercises that can reduce friction and help steer the right resources to the right places at the right time to keep attackers at bay.

> *“Collaboration across all teams, both offensive and defensive, is critical to ensure that organizations stay focused on resolving their most critical vulnerabilities. Organizations that focus on collaborative exercises through purple teaming and adversarial simulation are improving their security posture faster and with greater visibility.”* –Dan DeCloss, Founder/CEO of PlexTrac, Inc.

RESEARCH METHODOLOGY

In September 2021, CyberRisk Alliance conducted an online survey among 315 IT and cybersecurity decision-makers and influencers about their experiences with specific types of penetration testing models known as adversarial attack simulations and emulations (AASEs). Respondents were about evenly split between the United States (49%) and Canada (51%). Most (65%) worked at organizations with 1,000 or more employees, while the remaining 35% worked with smaller workforces (500 to 999 employees). Those surveyed worked in a variety of industries, including IT, financial services, industrials, energy/utilities, healthcare and life sciences, retail, professional services, education, government, media, transportation, hospitality and agriculture. The study was underwritten by PlexTrac.

Survey objectives were to understand current usage of AASEs, particularly how a traditional penetration testing model compared with the emerging purple teaming model. Researchers asked about adoption rates, trends, key drivers, common barriers, and plans to help gauge the popularity of both types, particularly in the wake of rising ransomware attacks. Study participants provided their responses to structured survey questions and were encouraged to submit corresponding comments where applicable.

EXECUTIVE SUMMARY

The power of purple teaming as a more effective alternative to traditional penetrating testing can be seen throughout the results of the CyberRisk Alliance survey. Respondents increasingly see it as a better way to vet existing tools, tactics, and procedures. It is also seen as a more effective way to help security decision makers steer their investments to the right places.

Though both types of AASEs challenge an organization's general cybersecurity readiness, including incident response and asset protection plans, purple team adoption was seen as adding several benefits, especially the prospect for improved collaboration between red and blue teams. Additionally, with the help of purple teaming platforms offering advanced features like artificial intelligence, machine learning and data analytics, survey respondents indicated they have used their purple teaming outcomes to lobby for more cybersecurity budget.

When asked specifically if their organization engaged in some type of AASE, almost half (45%) of survey participants said they had conducted

such exercises, whether penetration testing, purple teaming or both. Among the study's key findings:

- Purple teaming is gaining popularity, with more than one in four penetration testers having evaluated or trialed a purple teaming solution or approach and another third intending to give purple teaming a try in the coming year.
- The tech, industrial and financial services sectors were most experienced with purple teaming and use results to help shape their cybersecurity strategies, rather than just vetting current security controls.
- Even with a more strategic emphasis, almost 9 out of 10 purple team users found the exercises "very effective" in defending their organizations against ransomware and other advanced attacks.
- While both types of AASE users expected a reduction in future attacks because of exercises, purple teamers were more likely (88%) to believe their cybersecurity defenses had improved, compared to those using only penetration testing (52%). Their programs appeared to be more strategic, using results to advocate for more resources, talent, and tools than those who don't conduct purple teaming exercises.
- Among the top challenges for penetration testing adopters are siloed data and the inability to apply data analytics, limited resources to conduct exercises and a process that takes too long.
- Two-thirds of existing purple teaming users intend to invest more budget into this approach in the coming 12 months.

A MORE COLLABORATIVE APPROACH TO ADDRESSING THREATS

For decades, organizations have gauged their cybersecurity readiness with traditional penetration testing exercises involving red teams vs. blue teams. A red team is tasked with mimicking threat actors' known tactics, techniques, and procedures to launch an attack against an organization's IT infrastructure. It's up to blue team players to hold off such an attack with the resources on hand. A red team's win points to one or more vulnerabilities that must be addressed. Like traditional war games, no actual harm occurs. Instead, the exercises help everyone find and fix weaknesses in current security controls.

Such penetration testing exercises are seen as safe, competitive programs to discover flaws and establish remediations before an actual malicious attacker can break in and spy, steal or extort. But just as

threats continue to evolve, so too are these color-coordinated attack emulations to validate what's working — and what's not. Pentesting teams are now starting to come together to create purple teaming, which is built on a more collaborative model.

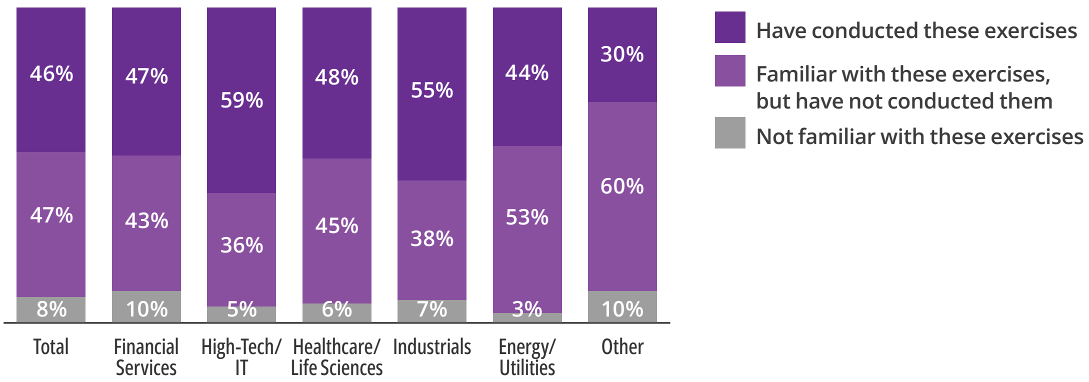
With purple teaming, attack modes and defenses are pre-determined. Both red and blue team members work alongside each other to test controls in real time and together learn how an attacker is most likely to gain illegal access by what works — and what doesn't.

Thought of another way: purple teaming is like a sports team scrimmage. Players are assigned opposing roles in a group exercise to anticipate future opponents' offensive and defensive plays while there's still time to change strategies and tactics. In testing each other's skills and technological protections, IT professionals together improve their overall security posture. And they are more truthful with each other, since sharing works better than depriving teammates of vital information.

THE MOVE TO PURPLE TEAMING

The increasing sophistication of attacks and growing complexity of IT environments is forcing security operations and the executives that oversee them to invest more resources than ever before. One way those surveyed appeared to benefit from AASE exercises, particularly purple teaming users, was in determining where to place future cyber investments.

Familiarity with Adversarial Attack Emulation/Simulation Exercises, by Industry Group



Q: What is your organization's familiarity and/or experience with conducting adversarial attack emulation/simulation exercises?

Nearly half of the North American IT security and cybersecurity decision-makers and influencers surveyed have conducted AASE (purple teaming and/or penetration testing) exercises. They represent a variety of industries but consist primarily of companies in information technology, financial services, industrials, energy, healthcare, and life sciences. A smaller group (including retail, education, government, media, transportation, hospitality, and agriculture organizations) was least likely to have conducted AASE exercises.

Both the tech and financial services industries tend to be early adopters of emerging cybersecurity technologies, given the potential damage to bottom lines and reputations should these solutions and service providers succumb to a malicious attack. So, it's no surprise these sectors had higher AASE adoption rates (59% for tech and 47% for financial services).

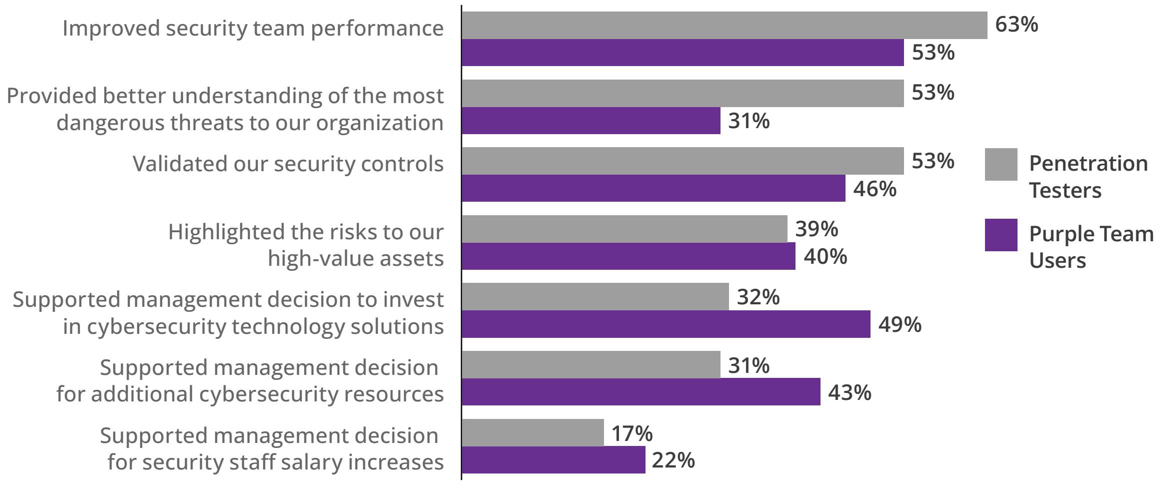
What may be more surprising is the industry with the second-highest AASE adoption rate: industrials (55%). This sector comprises manufacturing and goods distributors and reflects attackers' current focus on disrupting national and global supply chains rather than exposing pilfered databases on the dark web. The ransomware gang REvil, for instance, is widely believed to be behind the Colonial Pipeline attack in May 2021 that caused fuel shortages along the eastern United States. Around the same time, the same band of cybercriminals demanded $11 million in ransom to unlock systems belonging to JBS Holdings, Inc., which is responsible for a fifth of the U.S. meat supply.

PURPLE TEAMING MORE STRATEGIC THAN TACTICAL

The biggest benefits were more likely to be tactical for traditional penetration testers and strategic for purple teaming users. As a result of their purple teaming activities, security teams were more likely to acquire and allocate the right resources where they are most needed – both in terms of headcount and cybersecurity tools.

"By accurately simulating common threat scenarios and promoting the creation of new technologies aimed at preventing and detecting new threats, [purple teaming] helps the security team improve the effectiveness of vulnerability detection, threat search and network monitoring," said an IT security director for a U.S. technology company.

Top Outcomes of Attack Emulation/Simulation Exercises



Q: What have been the top outcomes of your adversarial attack emulation/simulation exercises? (Select up to 3)

Most purple teaming users primarily built exercises with a specialized purple teaming platform (89%) or breach and attack simulation (BAS) platform (80%) vs. 68% of BAS platform usage by red-team blue team users.

While both types of AASE users saw improvements in their security team performance as the top outcome, purple teams were more likely to gain management support for cybersecurity investments and secure more cybersecurity resources. Traditional penetration testers, on the other hand, better understood their biggest threats and performance of current security controls.

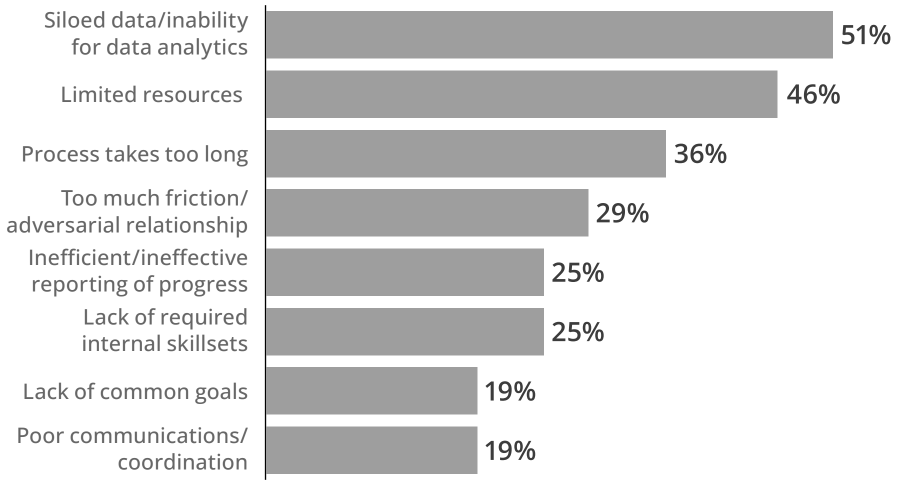
Research also found penetration testers were more likely driven to reduce attack volumes, while purple teaming users were in search of ways to reduce costs without compromising the organization’s cybersecurity posture.

“Our organization is very satisfied with purple teaming because we believe that together we can work toward a shared goal, which is the effectiveness of cybersecurity,” noted an IT security director for a Canadian industrial company.

CURRENT CHALLENGES WITH MANAGING DATA

Despite the maturity of penetration testing, users reported several challenges planning, designing or conducting exercises. Chief among them is how to analyze data to create actionable results.

Penetration Testing Challenges



Q: What are your organization's top challenges in planning, designing or conducting adversarial attack emulation/simulation exercises? (Select all that apply)

About half (51%) of penetration testers cited siloed data and the inability for data analytics as their top challenges, along with limited resources (46%). Other barriers included the extensive time involved or friction among players.

These responses reflect the need for outside expertise to launch and sustain such AASE programs and pull together accurate, accessible findings. Without timely data, remediation efforts may stall — thereby defeating the prime purpose of such simulations: to find and fix weak security controls.

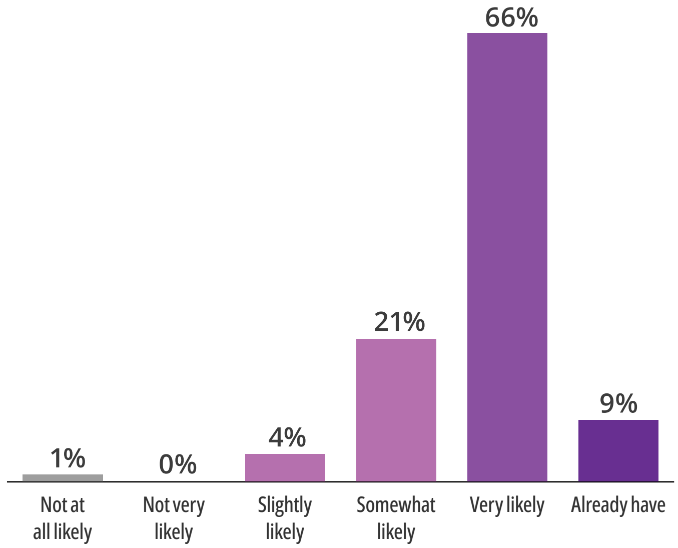
A MORE PURPLE FUTURE

Survey findings confirm growing interest in purple teaming as an expansion or replacement for the more traditional penetration testing approach. Among those who've conducted purple teaming, a large majority (88%) had also conducted traditional penetration testing exercises while only 3% said they have conducted purple teaming exclusively.

The latter, while a small number, shows that it's possible to launch a purple teaming program without penetration testing experience.

More than a quarter (27%) of current penetration testers indicated they have evaluated or piloted a purple teaming solution, and another 56% are looking into options. On average, those who currently conduct

Likelihood to Budget for or Invest in Purple Teaming



Q: How likely is your organization to budget for or invest in a purple team solution in the next 12 months?

penetration testing exercises anticipate allocating 16% of their IT security spend on AASE programs in the next 12 months.

Furthermore, given the high satisfaction rates among purple teaming users — 66% were very satisfied and another 32% somewhat satisfied — it shouldn't be surprising that 66% were very likely to budget for purple teaming solutions in the coming year. Another quarter were somewhat or slightly likely to do the same.

Based on respondents' feedback, it's easy to see why these companies are seeing a more purple future.

"My organization has had a good overall experience with purple teaming," noted a U.S.-based IT security director in the industrials sector. "It helps us achieve more effective vulnerability detection. Also, it fosters a healthier cybersecurity culture."

Another survey respondent from the financial services sector summed it up best: ***"Purple teaming's been wonderful in creating an atmosphere of collaboration amongst our team, especially during this period of remote working. Skills are honed and the team becomes real again to one another. Our ability to stop attacks has markedly increased, and it's been an unquestionable positive development."***

ABOUT CYBERRISK ALLIANCE

CyberRisk Alliance (CRA) is a business intelligence company serving the high growth, rapidly evolving cybersecurity community with a diversified portfolio of services that inform, educate, build community and inspire an efficient marketplace. Our trusted information leverages a unique network of journalists, analysts and influencers, policymakers and practitioners. CRA's brands include SC Media, Security Weekly, InfoSec World, Cybersecurity Collaboration Forum, our research unit CRA Business Intelligence, and the peer-to-peer CISO membership network, Cybersecurity Collaborative. More information is available at ***http://cyberriskalliance.com/***.

ABOUT PLEXTRAC

PlexTrac, Inc. is a fast-growing cybersecurity company driven by a mission to improve the security posture of organizations and security teams of all sizes. The PlexTrac solution is a software platform focused on streamlining the reporting and remediation of cybersecurity risks and aiding efficient collaboration within security teams. Supporting organizations using a purple teaming paradigm, PlexTrac serves as the central communication hub to aggregate all of the components of an organization's cybersecurity program. Visit ***https://plextrac.com*** for more information.