Cymulate

The Purple Highway to Risk Reduction

How Blue and Red Teams collaborate to bolster security posture

Cymulate

Table of Contents

Introduction

Today, every organization, regardless of its size, industry, or resources, needs to have access to both a red and blue team expertise and ensure they work together as a purple team to effectively combat cyber threats. With the cost of cybercrime reaching $1.79 per minute it does not matter if your sector is BSFI, healthcare, manufacturing, retail, critical infrastructure, technology, or any other vertical; integrating proactive approaches such as purple teaming is becoming a necessity to stay ahead of threats, patch the correct vulnerabilities on time and prevent security drift.

Purple teaming is often perceived as reserved for organizations with deep pockets, large staff, and highly cybersecurity skill sets. Automating a large part of the process with emerging technologies, as described in the “Automating Purple Teaming” and “Automated

Purple Teaming in Action” sections, now make it accessible to even small SOC teams with only blue teamers. A blue team is an integral part of an organization's SOC. It should have an inside-out understanding of the organization's infrastructure, a keen awareness of its objectives, and exhaustive knowledge of its assets and relative value. Their activity is focused on defending those assets from internal and external attacks. Their weapons of choice are monitoring all information traffic, detecting unusual activity, internal and external network vulnerability scans, DNS audits, etc. With the information gathered, they reactively adjust security controls configuration, PAM (Privileged Access Management) policies, and more.

At the other end of the spectrum, whether outsourced or as part of the SOC in-house resources, a red team activity covers all adversarial capabilities. They launch attack scenarios based on an embedded agent, or campaigns, fully outside-in attacks with no embedded agents, to identify points of entry and vulnerable attack paths within the organization's infrastructure and networks.

Unfortunately, though blue team capabilities are typically maximized within an organization, reliance on the red team can be limited to a desire to satisfy compliance regulators without a thought to the actual security impact of inadequate red teaming exercises. This risks leading to situations where red teamers feel they are not given adequate resources or help from the blue team in their testing. Blue teamers might perceive red teamers as a distraction, question their assessment accuracy or relevance, or criticize the lack of adequate feedback on what to fix and how.

Practically, this means that a red team can be as minimal as an outsourced annual penetration testing exercise, sometimes still even performed manually. Those periodic penetration tests are only ever as good as the person launching it, as humans are susceptible to limitations in time, scope, skills, distractions, emotions, and, in some cases, bias. The resulting report will be used as a reference document by the blue team until the next exercise a year later, by which time it is woefully outdated. With the rapid relevance obsolescence of periodic red team assessment, annual or even quarterly outsourced red team exercises, though they might still satisfy compliance regulators, are inefficient in providing timely actionable information.

This sorry state is predominantly due to a lack of resources, an issue that can effectively be tackled through automated purple teaming. This eBook first examines in depth the rationale behind adopting purple teaming before reviewing the lesser-known managerial benefits of adopting it, then continues to delineate the requirements and, finally, explores a practical integration and automation of purple teaming.

What is Purple Teaming?

A purple team brings together a red and a blue team to combine their adversarial and defensive skills. Purple teaming is the process of getting these two teams to collaborate and work together.

When blue and red teams work separately, each team focuses on its specific area of expertise.

- Red teams launch harmless attacks to uncover weaknesses, exploitable vulnerabilities, and other security gaps.
- Blue teams scan the infrastructure for weaknesses, vulnerabilities, and other security gaps, mitigate those and monitor the infrastructure to detect and stop attempted attacks.

In this model, red teams try their best to bypass the defensive mechanism erected by the blue teams and avoid detection, and blue teams feel threatened by red team success. When working separately, red teams are often perceived by blue teams as finding all the flaws without effectively educating and prescriptively providing feedback on how to fix and remediate. On the flip side, red teams typically lack a comprehensive understanding of the infrastructure, and their security validation process might lack depth and thoroughness.

Ideally, merging those two teams into a single purple one eliminates those antagonizing aspects and fosters collaboration. By working hand in hand with the red team, the blue team gets new insights into the adversarial rationale behind security gaps and misconfigurations, enabling them to prioritize remediation better, thus hardening the overall security posture without additional resources. As a bonus, the blue team can include in-context justifications and, ideally, actionable mitigation recommendations, in the security-based requests sent to the IT team, reducing friction between SOC and IT teams. Purple teaming combines the capabilities and knowledge of both blue and red teams. When collaborating, the information these two teams can gather with the right framework empowers security professionals and leaders to manage, know and control their cybersecurity posture end-to-end and achieve near real-time closing of identified security gaps.

Purple teaming's ultimate goal then becomes to acquire the ability to visualize, understand and analyze all elements of your security posture from both defensive and offensive perspectives, providing overarching confidence in making decisions about the optimal actions to take to solidify that security posture and prevent security drift, while allowing for business operation optimization.

Why Purple Teaming?

Behind purple teaming's primary purpose of hardening the overall security posture, purple teaming saves time and resources and optimizes not only the infrastructure security but also related internal communication and collaboration across previously segregated departments.

01

Saving time

With segregated blue and red teams, the sequential nature of information flow slows down the mitigation process. The red team identifies and lists securities gaps and sends the list to the blue team. The blue team then needs to:

- Contextualize each gap
- Understand the rationale explaining why each gap creates a security risk
- Define the appropriate mitigation process required
- Send it to the IT team for implementation

When purple teaming, the process is considerably shorter as the red team conveys both the context and the rationale, often shortening the mitigation process creation. This leaves only two steps instead of four.

02

Accelerating risk reduction

Combining adversarial and defensive perspectives enables a far better documented understanding of the efficacy of the SOC tool stack. When solutions are bought based on vendors' descriptions and minimally configured, it often results in a tool sprawl with underutilized resources and unintelligible data. Purple teaming identifies ill-configured, under-used, ineffective, missing, or overlapping solutions.

03

Saving resources

Rationalizing and reconfiguring the defensive tool stack based on the information gathered through purple teaming not only directly increases cybersecurity solutions ROI, it also reduces the number of false alerts and the related risk of alert fatigue. It streamlines analysts' data flow, thus improving their output accuracy and timeliness.

04

Optimizing internal communication and collaboration

The ability to measure the security infrastructure resilience based on its ability to withstand a comprehensive array of attacks generates accurate metrics and definitive answers to specific questions that replace prior guesstimates based on adherence to best practices. This provides a new level of visibility into risk exposure that facilitates communication between the executive and technical departments and cements collaboration. It also eliminates the antagonism between blue and red teams, replacing it with a single team with better-combined knowledge and skill set.

Purple teaming focuses on hardening the security posture far beyond the basic requirement of checking boxes for compliance purposes. At its core, purple teaming combines a blue team's traditional reactive defensive methods with the insights gained from proactive offensive validation techniques typically used by penetration testers and red teams. The resulting assessments are far more thorough, and the blue and red team collaboration from the start promotes a smooth implementation of the uncovered required mitigations.

When run in tandem with continuous security validation techniques, purple teaming integrated with day-to-day IT and DevOps deployments acts as an enabler by accelerating business goals while simultaneously reducing risk.

Is Purple Teaming Relevant for you?

To evaluate how critical adding purple teaming capabilities is for you, it might be useful to ask a few questions about the relevance of purple teaming for your organization, given your existing security infrastructure.

Asking the right questions

So, let's start by looking at the questions that might justify opting for purple teaming when looking at the security validation options.

01

Is compliance the main reason you are running pen testing/red teaming exercises or is it to improve your security?

Even if satisfying the regulators might limit the fines for non-compliance, it will not deter malicious actors from launching attacks, and, if successful, these attacks might carry heavy costs ranging from loss of IP to damages to users and, of course, all the cost associated with business interruption, reputational damages, loss of clients, etc.

If your goal is to improve security, then periodic pen testing or red teaming exercises will only go so far:

- The combination of the frequent deployments inherent to agile development, each of which might introduce new security gaps, and the constant emergence of new vulnerabilities – and related exploits - and new threats renders periodic validation exercises obsolete almost as soon as the report is handed in.
- Penetration test quality varies as testing is only as good as the person coming to do it, is limited in time and scope, and can even be exploited by the testing company to ensure future business.
- The lack of built-in collaboration between your blue team and the in-house or outsourced validation teams is likely to create friction and result in siloed, potentially antagonistic teams.

02

Are you buying additional defensive solutions because you have the budget or because they add a significant delta to your security readiness?

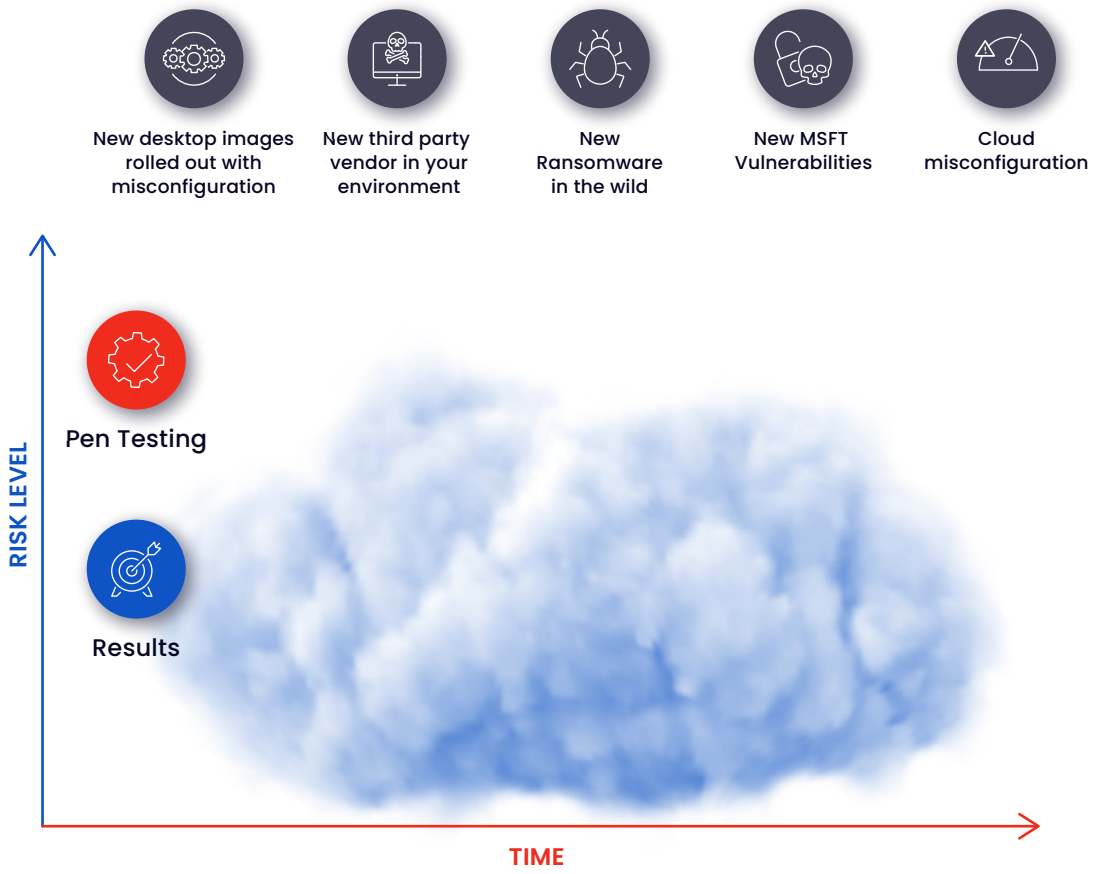
As news of catastrophic breaches is becoming a staple of the regular newscast, awareness of the potential cost of such breaches resulted in a growth of the cybersecurity budget. The chronic shortage of skilled cybersecurity professionals is nowhere near being solved; it is tempting to rush to buy new tools, preferably with AI, ML, and lots of automation to shore up security. Yet, the problems with adding new tools are that:

- Vendors' POC tests are seldom genuine – When a vendor offers to run a PoC of its solution, it is often biased, so testing their efficiency should be performed by a third party such as Cymulate.
- Despite the vendors' marketing material, they are rarely truly plug-and-forget - Though some level of added security might be added using the tool as-is, each of these new tools needs to be configured individually and collectively to activate their full potential.
- Adding tools increases complexity – Each of these new tools produces data. Collating, organizing, and analyzing that data emanating from numerous sources and translating it into informative insights and actionable decisions become more complicated and less likely as the data mass grows. To add insult to injury, ill-configured tools with adjacent or overlapping capabilities sometimes generate contradictory results.
- More tools mean more alerts – Not only are additional tools adding complexity, but they also risk increasing the number of alerts, hence alert fatigue, and the resulting risk of ignoring valid ones.

So, defining which tool to add and why using the relevant data harmonized across blue and red teams is critical to selecting the right tools. A bonus of focusing on optimizing and rationalizing the solutions array instead of adding more to it is that it might lead to eliminating overlapping tools and redirecting that budget to tools offering erstwhile undetected missing capabilities.

03

Can you monitor and preempt security drift?



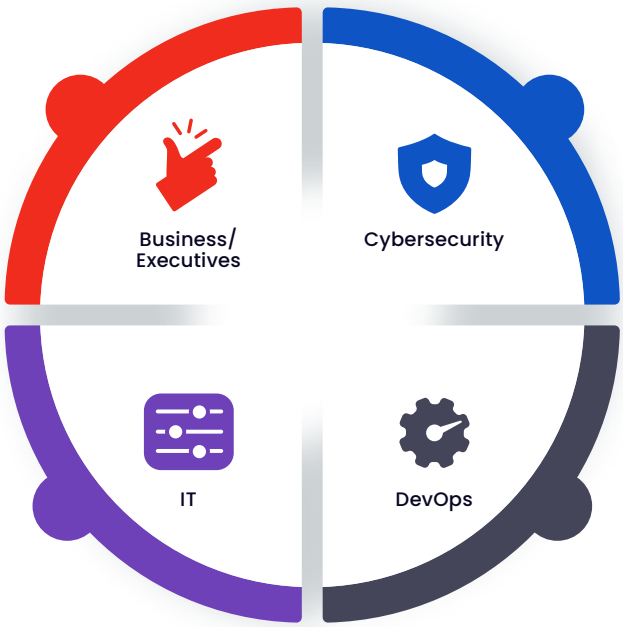
Security drift is what happens when you are not looking. When red teaming or pen testing exercises are only performed periodically, the tendency is to rely on the estimated security posture at validation time and assume it is stable until the next validation station.
Yet, as both the cyber-threat landscape and your environment architecture are in constant evolution, this reliance on static data is dangerously misleading.

In today's constantly shifting reality, the risk of drifting from a secure security posture into a perilous one can only be avoided through continuous security validation and recalibration of security controls based on hard data. Continuous testing provides the assurance that traditional testing methodologies cannot.

Purple Teaming Additional Benefits

With a better idea of the underlying reasons behind the decision to adopt purple teaming, we can now explore more in-depth the additional benefits derived from the purple teaming built-in effect of breaking down the walls between cybersecurity, IT & DevOps, and business/executive teams.

Breaking the Communication Walls between Security, IT, DevOps, and Business



Though at first glance, purple teaming seems to be the result of combining two teams, in fact, it is closer to reality to say that it combines four. Traditionally, despite the common goal of advancing the organization's goals, cyber , IT, DevOps, and business executive teams work at cross-purposes. Let's have a look at the intermediate priorities of each of the three teams that might lead to creating walls between the teams:

01

Security

Cybersecurity teams are focused on securing the infrastructure and, as such, are alert to the lurking dangers and the need to prioritize closing all the security gaps over the need to perform. They have to bridge "technology" and "risk" and walk the thin line between maintaining operability and protecting business executives from the aftermath of a catastrophic breach.

02

IT

When it comes to configuring their organization endpoints, IT teams are sitting at the junction of conflicting priorities.
Sandwiched between employees resistant to curtail their Internet surfing, social messaging, and other online activities, DevOps wanting maximum flexibility with servers, PaaS, IaaS, and more, and cybersecurity teams keen on securing endpoints at any costs, IT teams have to walk a thin line to avoid conflicts.

03

DevOps

DevOps teams love creating new software that works. They would rather have their software deployed today without any "security equipment" than invest time in tightening Privileged Access Management, scanning images for vulnerabilities, or dot their i's and cross their t's when configuring security controls.
Furthermore, they face intense business pressure as executives want them to do more and want it two weeks ago.
This increases pressure and leads to resentment against cybersecurity requirements that slow down the deployment cadence.

04

Business

Business decision-makers and executives want everything to run smoothly with zero business interruption, ever-happy users, and satisfied regulators. Despite their limited mastery of the technologies involved, they are the ones tasked with arbitrating between the Cyber and IT/DevOps teams and risk getting influenced by the most articulate team leader regardless of the value of their argument.

These goals are often conflicting, and finding the right balance to define the optimal path requires each side to fully understand the other priorities, obligations, and limitations. Without such an encompassing understanding, one side might insist on the other side “drawing a circle with corners.”

Purple Teaming – The Fastest Lane to Success

To harmonize those conflicting goals, all teams must work in unison. In other words, the first step is to define a common ground that considers the need of all players. As purple teaming encompasses both the defensive and the adversarial validation of risk assessments, security priorities are firmly established, including streamlining vulnerability patching, which lightens the load of the IT team. The resulting harmonized and documented goals shared by the cyber and IT teams facilitate communication with executives.
Detailing the effect of purple teaming on each group gives a more in-depth understanding of purple teaming full impact:

01

Security

As blue teams integrate adversarial technologies or red teams into purple teaming, the immediate effects are:

Cybersecurity teams are focused on securing the infrastructure and, as such, are alert to the lurking dangers and the need to prioritize closing all the security gaps over the need to perform. They have to bridge "technology" and "risk" and walk the thin line between maintaining operability and protecting business executives from the aftermath of a catastrophic breach.

As blue teams integrate adversarial technologies or red teams into purple teaming, the immediate effects are:

- Homogenizing cybersecurity data – with data stemming from a direct measurement of the blue team's ability to preempt, stop or mitigate attacks, measuring cybersecurity posture can be harmonized and rely on hard data instead of the typical guesstimate of a purely blue team.
- Providing comprehensive, quantified, transparent, and up-to-date visibility of the security posture – When purple teaming is fully incorporated into the daily cybersecurity routine, the exact nature of the measurement yielded is ideal for measuring baseline and tracking trends and variance from baseline.
- Improved understanding of IT missions and pain points – When attacks are comprehensively emulated, identifying which attacks are detected and what corrective measures are taken facilitates the prioritization of vulnerability patching, as even high score vulnerabilities can be deprioritized when security controls are configured well enough to protect the infrastructure from the risk posed by that vulnerability.
  Conversely, lower CVSS scored CVEs can be pushed higher in the patching schedule if they are identified as posing a higher risk. When the IT team sees clearly the rationale behind an emergency patching request and knows that those are kept to a documented minimum, they are far more likely to react swiftly.
- Incorporation of IT priorities and limitations in mitigation strategy – Conversely, as blue and red teams work in tandem with the IT/DevOps team and executives, they become aware of the IT/DevOps team's pain points and of the impact of security-based decisions on the organization operations and can incorporate these data in their decision-making process from the start, preventing frictions down the line.
- Improved collaboration between teams -As a direct result of the improved understanding of each team's priorities and pain points, collaboration replaces previously antagonistic siloed teams.
- Shifting further left of the security as it is incorporated into IT and DevOps processes – the combination of more accurate data, better prioritization, and goal convergence results in easing the early incorporation of security in the development process, which improves security and accelerates the overall development process.

02

IT

The ability to discuss their priorities directly with the security teams leads to a better mutual understanding and yields positive results:

- Provides data to prove the value of IT spend
- Enforces network segmentation policies
- Documents the rationale behind imposed access and privileges restrictions

03

DevOps

As they are included from the beginning in the security posture solidification process, and as the red and blue teams' collaboration translates into streamlined mitigation with a demonstrated effect, DevOps teams :

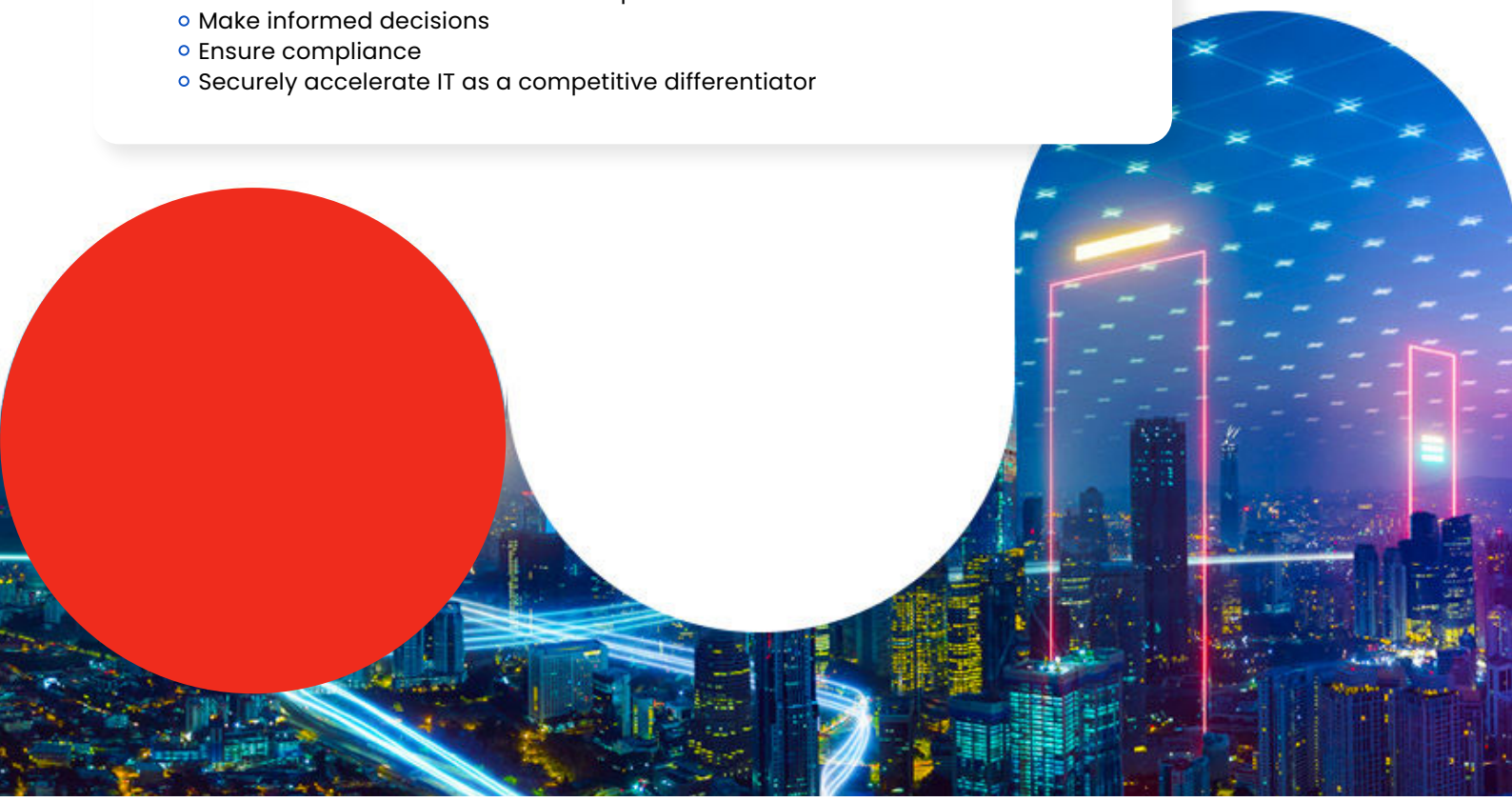
- Visualize and understand the risk implications
- Make informed decisions
- Ensure compliance
- Securely accelerate IT as a competitive differentiator

04

Business

With the cybersecurity and the IT department working hands in hands with tools that provide a comprehensive, quantified, and up-to-date overview of all security posture aspects, business decision-makers and executives can.

- Visualize and understand the risk implications
- Make informed decisions
- Ensure compliance
- Securely accelerate IT as a competitive differentiator

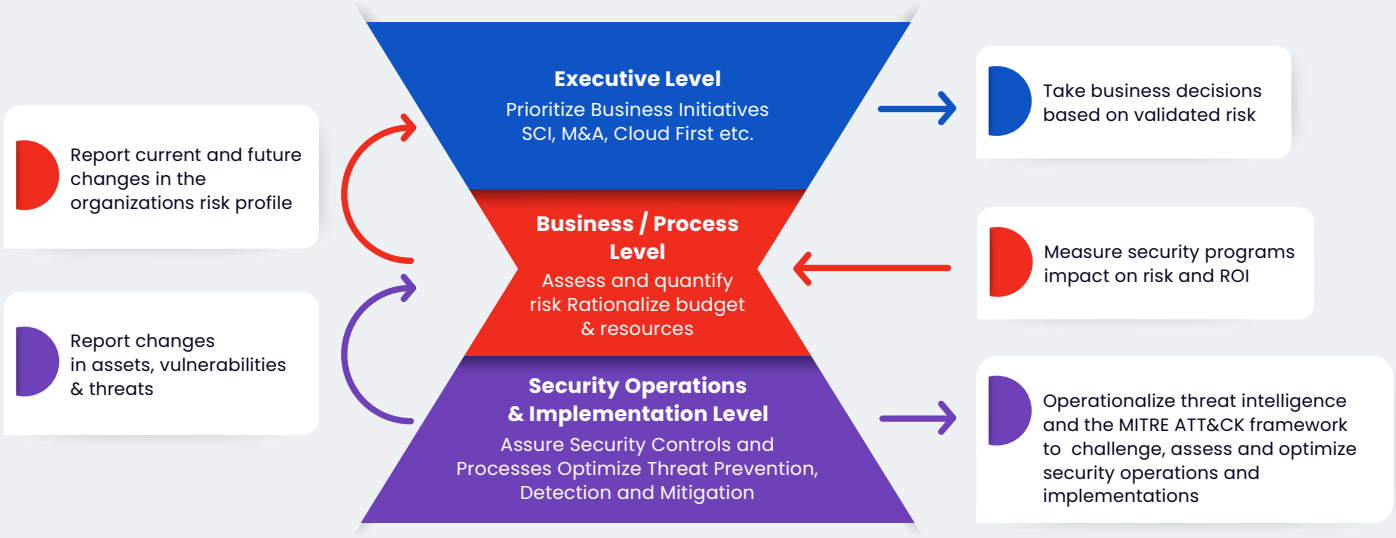


Purple Teaming in Extended Security Posture Management

The power of Purple Teaming's ability to create templates to run chained or atomic assessments can be further enhanced by incorporating it into an Extended Security Posture Management (XSPM) platform.
XSPM, short for Extended Security Posture Management, is a continuous security assurance program that maximizes operational efficiency while minimizing risk exposure.
Cymulate's XSPM comprehensive platform covers the entire kill chain from recon to extraction and command execution with a set of technologies described in detail in XSPM's overview ebook. Its extensive capabilities help manage exposure to cyber threats, map and block possible breach routes, and validate security controls' effectiveness.
Now that we have covered in detail how continuous purple teaming ties together Cybersecurity, IT, DevOps, and business executives, it is time to analyze how XSPM magnifies purple teaming. Aside from is available purple teaming advance framework that provides off-the-shelf templates and components to dynamically create custom assessments, Cymulate's XSPM platform provides a clear, understandable, and up-to-date view of the trending security posture, variance from baselines, and the general evolution of the security posture management.

The first step is establishing baselines that will serve as reference points to monitor and analyze trends. Baselines are defined in collaboration with the board and designed to match the organization's risk appetite and business goals. Ideally, baselines should be established granularly according to priorities. Once the initial set of baselines is defined and the purple team sets up the relevant automation to ensure continuous validation of the parameters underlying the baselines.

Used to Convey Risk Accurately and Timely



The graph above visually shows how XSPM integrates the interactions between defensive (blue), adversarial (Red), and combined (purple) capabilities to accurately and timely measure ad define risks and their potential business impact. As the cycle is recursive and an organization's main goal is to maximize its business or processes objectives, we will start by looking at how the security operations and implementation level affects the business/process level.

01 At the security operations and implementation level, the purple team runs comprehensive end-to-end attack scenarios and campaigns to assess security controls configuration effectiveness in compensating for detected CVEs, evaluating the impermeability of segmentation between processes, and optimizing threat prevention and detection and mitigation.

02 The purple team then reports any modification in the risk exposure, whether stemming from changes in assets, the emergence of new vulnerabilities due to internal changes or recently uncovered vulnerabilities in the wild, and resilience to new threats.

03 These modifications are correlated with related baselines to measure trending and prevent security drift.

04 This information is integrated at the business/process level.

05 At the business/process level, this information is leveraged to

a. Assess and quantify the risk in a format designed to transparently inform the executive level with fact-based metrics and without relying on complex technical explanations.

b. Measure the efficacy of the existing security programs, evaluates the solutions continued effectiveness, and take proactive measure to rationalize the tools stack to eliminate overlapping capabilities and re-affect resources to missing ones.

06 Upon receiving itemized reports about the current state and the foreseeable evolution of the organization's risk profile, the executive level makes informed decisions and prioritizes business initiatives with minimal risk of endangering the organization.

07 The security impact of these new initiatives is automatically evaluated as they are implemented, and the security operation and implementation level produce updated reports that follow the same process, and the cycle starts again.

This continuous cycle enables a clear view of the security posture at any time and prevents security drift.

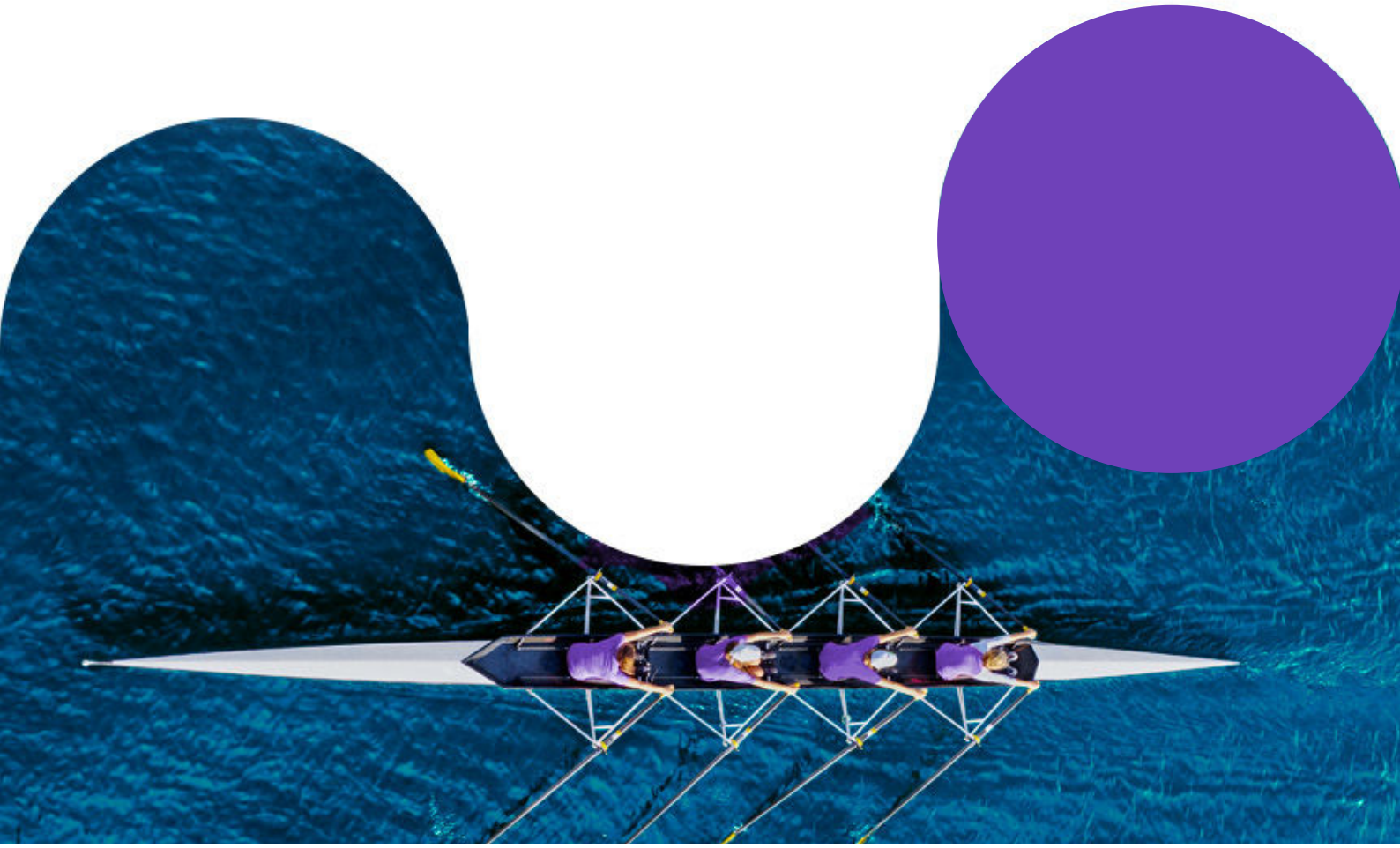
Automating Purple Teaming

The best way to continuously enable purple teaming without massive resource increase is to automate a lion part of the process. This requires access to off-the-shelf technologies that enable automation and generate fact-based data with accurate metrics that can be easily correlated to facilitate analysts' work and with actionable mitigation recommendations to accelerate the remediation process.

Recommended Technology Capabilities

A purple teaming framework enabling automation should include:

- **Extensive scenario and campaign templates:** off-the-shelf templates cut down complex and tedious work so that your team can focus on testing and, if needed, further customizing templates to match the specifics of your environment
- **Scenario and campaigns creation wizard:** Even with a large collection of available templates, there is likely to always be a need to create entirely new scenarios or campaigns. A framework should include a wizard with ready access to a comprehensive array of attack, execution, delivery, and spreading methods, evasion techniques, and all constitutive attack elements. This way, your team can simply combine the off-the-shelf elements into a specific attack scenario or campaign instead of having to encode each element separately.



- **Scenario and campaigns creation wizard:** Even with a large collection of available templates, there is likely to always be a need to create entirely new scenarios or campaigns. A framework should include a wizard with ready access to a comprehensive array of attack, execution, delivery, and spreading methods, evasion techniques, and all constitutive attack elements. This way, your team can simply combine the off-the-shelf elements into a specific attack scenario or campaign instead of having to encode each element separately.

- **Access to Immediate Threat Intelligence (ITI):** the framework should be integrated with a continuously updated source of actionable information about emerging threats that can be used to create attack scenarios or campaigns as soon as a new threat emerges. ITI capabilities should:
  - Include the option to automatically update daily based on the latest IoCs and TTPs because it is impossible to update this manually without considerably increasing the staff
  - Accommodate the changes in infrastructure following new deployments
  - Be flexible enough to integrate the shift of baselines due to changes in business goals

- **Comprehensive testing options:** the off-the-shelf templates and the wizard capabilities should cover agent-based testing scenarios that validate security controls configurations as well as outside-in attacks that mimic attackers' attack path from initial foothold to mission execution (exfiltration, command execution, or other). Ideally, this means already integrated technologies such as
  - External Attack Surface Management (ASM) to detect attackers scanning your environment, the internet, and the darknet for assistance in gaining an initial foothold
  - Phishing campaign creation and execution capabilities to continuously validate your employees' alertness through phishing campaigns enable identifying weak links and remedial awareness classes targeting employees who fall for the fake phishing message.

- **In-depth analytics capabilities:** No two organizations are the same, and each needs to correlate different sets of data to extract the information they need. This requires flexibility in the options to select specific data sets, scope, and duration and visualize the findings uncovered through correlation in a variety of display options ranging from simply numeral display to graphs, charts, tables, and more.

- **Detailed output:** The findings need to include:
  - Visibility into risk through granularly mapping risk exposure across the entire kill-chain.
  - Prescriptive remediation outputs that not only provide actionable remediation recommendations but also evaluate SIEM and SOAR tool stack efficacy by identifying overlapping and missing capabilities and pointing out how to optimize their performance.
  - Vulnerability Prioritization Technology such as Attack Based Vulnerability Management (ABVM) to detect and assess vulnerabilities' risk to your specific environment and evaluate the effectiveness of compensating security controls, ultimately leading to a significant reduction of the patching workload.

The added benefit of relying on an advanced purple teaming framework that includes those capabilities is that it makes purple teaming accessible to teams of cyber professionals of any cyber-maturity levels, from beginners who rely heavily on off-the-shelf automation and pre-encoded prescriptive explanations to experts keen on maximizing advanced automation options and customize templates.

Cymulate Automated Purple Teaming Overview

This constellation of capabilities is included in Cymulate's Extended Security Posture Management (XSPM) platform. The platform has built-in libraries of assessments, scenarios, individual attacks, and deactivated payloads across a comprehensive array of execution methods, turning the platform into a de facto purple teaming framework.

Get a preview of the platform, download the XSPM Overview eBook!

About Cymulate

Cymulate was established with the vision of empowering security professionals to make better decisions faster, based on real-time data. Founded and led by an elite team of cyber researchers with world-class experience in offensive cyber solutions, Cymulate is determined to become the golden standard for security professionals and leaders to know, control, and optimize their cybersecurity posture end to end. Trusted by hundreds of companies worldwide, Cymulate constantly enhances its methods to prepare organizations for any attack scenario or campaign.
With Cymulate, organizations continuously measure security performance in real-time, shore up defenses, and assure operational effectiveness.
Measuring your cybersecurity performance is fundamental towards creating a more secure organization!

Headquarters: Maze St 3, Tel Aviv 6578931, 7546302, Israel | +972 3 9030732 | info@cymulate.com