



mission
multiplier

Cybersecurity is Seeing “Purple”

*The rising movement to integrate cyber **Red** and **Blue** Teams to create a “**Purple Team**” capability; and to achieve greater integration with application developers*

December 2024

*This document contains Mission Multiplier Proprietary
and Confidential Business Information.*

1.0 INTRODUCTION

Headlines continue to be filled with reports of government agencies and large companies being victimized by cyber intrusions. This remains true despite a proliferation of cybersecurity guidance and large increases in cybersecurity spending (around \$150 billion per yearⁱ globally on cyber products and services). Why? In addition to increasingly well-financed threat actors, the “attack surface” where these attacks are deployed is changing dramatically.

- The number of applications used by a typical organization has rapidly grown over the last decade. According to the 2024 BetterCloud Report, a typical organization uses 130 SaaS apps, up from 16 apps five years ago. Each application requires an overall state of cybersecurity readiness, vulnerability management, and authentication controls.
- The number of internet of things (IoT) devices is also exploding -- some forecasts project that there will be 41.6 billion such devices by the end of 2025ⁱⁱ. And 5G networks will enable a much greater level of distributed computing at the edge. Drone and robotics are no longer simply the thing of military environments — they are being used today in many industries and service areas, from farming to retail distribution centers, to delivery services, and more.
- The software and firmware running these systems sit atop increasingly complex codebases, both in sheer size and dependency on third-party and open-source code. The original space shuttle’s code base was only 400,00 lines of code, while modern cars have over 100 million lines of code – which continue to grow as the code gets updated.

This new operating reality is forcing organizations to make major changes to how they set-up and deploy their cybersecurity programs, one of which is the **movement to integrate Cyber Red and Blue Teams to create a “Purple Team” capability and to achieve greater integration with application developers.**

2.0 OVERVIEW

A Purple Team is a hybrid team concept that combines the roles and functions of Red Teams (offensive) and Blue Teams (defensive) to enhance an organization’s overall cybersecurity posture. The idea behind a Purple Team is to facilitate better collaboration and information sharing between these traditionally separate teams, aiming to improve the effectiveness of both offensive and defensive security measures. The fundamental differences between a Blue, Red, and Purple Teams are captured in **Figure 1** below.

	Blue Team	Red Team	Purple Team
Scope	<ul style="list-style-type: none"> ▪ Involves defensive cybersecurity 	<ul style="list-style-type: none"> ▪ Involves offensive cybersecurity 	<ul style="list-style-type: none"> ▪ Integrates defensive and offensive cybersecurity teams
Objective	<ul style="list-style-type: none"> ▪ Defend against cyber threats 	<ul style="list-style-type: none"> ▪ Recreate known cyber TTPs in “the wild” and test impacts 	<ul style="list-style-type: none"> ▪ Connect defensive cyber procedures with offensive TTPs
Responsibility	<ul style="list-style-type: none"> ▪ Implement cybersecurity controls and processes 	<ul style="list-style-type: none"> ▪ Test the efficacy of cybersecurity controls based on known cyber TTPs along with cyber incident response capability 	<ul style="list-style-type: none"> ▪ Facilitate learning by conducting cross-training between blue and red teams.
Process	<ul style="list-style-type: none"> ▪ Monitor and improve cybersecurity controls and processes 	<ul style="list-style-type: none"> ▪ Determine the risk of enterprise to defend against TTPs 	<ul style="list-style-type: none"> ▪ Communication and training processes to facilitate learning and skills enhancement
Team	<ul style="list-style-type: none"> ▪ In-house or outsourced security monitoring and incident response 	<ul style="list-style-type: none"> ▪ In-house or outsourced ethical hackers, social engineers, and threat analysts 	<ul style="list-style-type: none"> ▪ Integration of blue and red teams through side-by-side training and simulations

Figure 1: Comparison Overview of Blue, Red, and Purple Teams

One of the fundamental areas that Purple Teams enable is supporting an organization’s cyber defenders and application owners so that they can keep pace with the latest tactics, techniques, and procedures (TTPs) of cyber adversaries. This is particularly important when organizations utilize and develop custom applications, configurations, application programming interfaces (APIs), and software – which nearly every organization relies on. The last thing that an organization wants is to spend a lot of time and resources on developing and implementing proprietary and custom applications/software and then having that software immediately, or near-immediately, compromised when it is released –nullifying the large and often strategic investment for a new solution.

To ensure that there is a meaningful return on investment for application/software development, it is necessary for application developers to continuously collaborate with cyber-Purple Teams, so that they can be trained (through side-by-side interactions and simulations) on how to address existing and emerging cyber vulnerabilities. By “building in” the appropriate security controls into applications and software while leveraging the Continuous Integration and Continuous Delivery (CI/DC) process, an organization can significantly reduce the risk that it will be compromised by the adversary.

The overall concept of how the integration of Blue, Red, and Purple Teams; and the application development teams can effectively work is captured in **Figure 2** below.

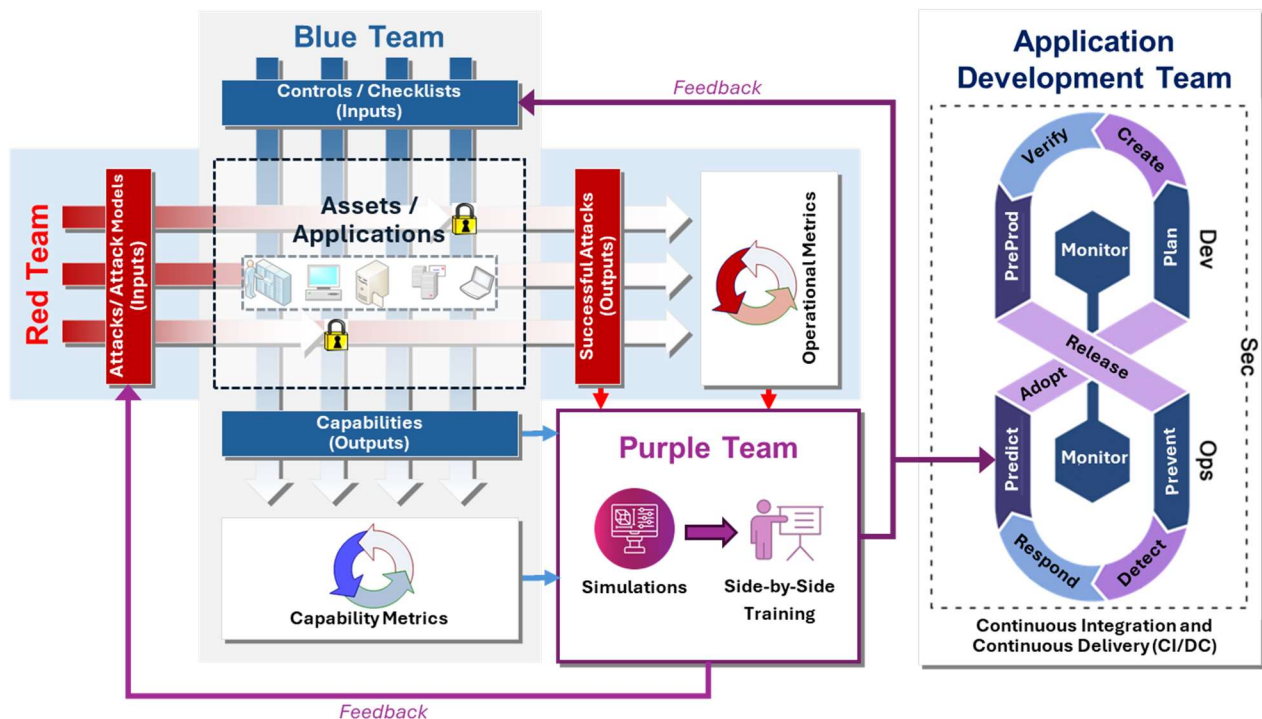


Figure 2: Integration Flow Between Red, Blue, Purple, and Application Development Teams

Continuously assessing technical IT security controls (Blue Teams), alongside the adjacent and continuous threat assessment (Red Teams) is critical to achieve effective enterprise risk management. However, it is not sufficient for Blue and Red Teams to work independently. To drive maximum value, they should work closely together. As Red Team assessors identify new and relevant threats, the impacts of those threats should be simulated on the respective organization’s network and applications;

and the cyber defenders (Blue Teams) and application developers (when appropriate) should be trained on how to better address the latest threats and vulnerabilities. By more fully understanding the impacts and “weak points” of the network, applications, or configurations, the Blue Team members and application developers can more effectively respond, and act more proactively to mitigate cyber risk.

3.0 BLUE TEAMS

Blue Teams are charged with on-going monitoring, scanning, and implementation of network, system, and IT security controls to address potential IT vulnerabilities, and then supporting any remediation activities to address the identified vulnerabilities. The required IT security controls derive from security standards, frameworks, regulatory obligations, and internal policies that are imposed on each respective organization. The adoption of new and emerging technology (e.g., cloud computing environments) contributes to further expansion of the “attack surface”, while also drives a growing number of IT security controls.

The Blue Team’s monitoring and scanning cadence is further derived from the organization’s risk tolerance, compliance mandates, and the number and type of IT assets managed. Blue Teams typically use and combine various scanning methods (for example, agent-based, network scanning and passive network devices) to achieve the desired scanning frequency. Critical assets are normally scanned more frequently, or even continuously; however, depending on the organization’s risk policy, less critical assets are scanned less frequently – weekly, monthly or quarterly. It is imperative that the rate of scanning is marginally higher than the rate of remediation, as the process should account for other activities (such as validation and implementation).

Given the proliferation of threats and threat actors, more effective and efficient monitoring and remediation cycles are needed. To achieve this result, Blue Teams can:

- Define accountability structures (i.e., ensure that Blue Team members, business owners, and application developers) fully understand their IT security roles and responsibilities.
- Promote collaboration with Red Teams to shorten and close the vulnerability detection and remediation loop.
- Conduct regular meetings with other business units (and system owners) to check the status of active vulnerabilities and guide stakeholders through possible roadblocks.
- Avoid treating all IT assets the same. Where possible, segregate environments based on criticality and compliance or, at a minimum, have policies that account for the difference.
- Pay attention to the business context of assets and threat exposure before running periodic discovery scans.
- Optimize resource utilization by focusing on addressing exposures to the most critical assets first.
- To the extent possible, integrate automated patch management solutions and the vulnerability scanning tools with built-in patch management solutions. Application-layer vulnerabilities are best managed leveraging a DevSecOps model, which integrates vulnerability tools with CI/CD cycles, so that code vulnerabilities can be fixed during the Agile development process.
- Work with Purple Teams to create and employ remediation run books to assist team members in taking prompt, corrective actions. Run books are a great way to enhance response actions. They aim

to automate approved and tested processes, which often create burdensome, manual overhead for Blue Teams when compounded with today’s vulnerability volumes.

- Work with Purple Teams to create and maintain remediation databases to add pace to the overall remediation cycle. The adoption of security orchestration, automation and response (SOAR) tools can support reproducible processes to be partially or wholly automated.

Although Blue Teams still play a crucial role in an organization’s network security, the key theme is for them to have more connectivity to key stakeholders – Red Teams, Purple Teams, and operational business units.

4.0 RED TEAMS

An organization’s use of Red Teams (or Threat Hunters) is a critical component to a successful security program. Red Teams provide organizations with an opportunity to test its Blue Team (defensive capabilities) against the techniques and approaches used during real breaches, to see how the IT controls fare and how the Blue Team reacts; as well as to identify areas of improvement. Red Team exercises give organizations the closest experience to the real attack to help improve its resilience, so they have a chance to address their vulnerabilities before they are compromised by potential adversaries.

Organizations must undertake a continuous assessment of where they are in terms of the maturity of their Blue/Red team capabilities. This ensures that they can maximize the time, resources and budget available to improve their risk posture. Security and risk management leaders in charge of security operations must understand that engagement with and use of on-going Red Teams is essential to improve cybersecurity resilience.

By employing Red Teams, organizations can use threat intelligence to understand the top threats that pose a significant risk to the business/mission. More specifically, Red Teams can formulate or simulate scenarios to determine potential impacts to the network, systems, and applications given a specific threat or TTP behaviors. Red Team deployment of threat simulations is key because it enables Blue Teams and application owners that opportunity to see the potential impact of changes, infrastructure deployments, and even code changes, in a safe (not-live) environment.

A Red Team allows for mistakes to be made preemptively so they are not made in a real disruptive event. Learning points can be used to build response procedures and updates to infrastructure and system-level configurations, leading to a more robust risk response that reduces business impacts and facilitates a more efficient return to normal business operations. Utilization of Red Teams provide:

- The opportunity to stress-test biases and assumptions.
- Better understanding the impacts of a breach and so that there is a reduction in the time from detection and recovery.
- More enhanced communication strategies to ensure that effective collaboration between key stakeholders regularly occur.
- Unique insights into how to better mitigate risk.

Time is of essence when managing the impact of a breach. Therefore, a shift toward proactive and collaborative communications between Red and Blue Teams (and application developers) is a must, as it helps enable the best use of available resources such as people, time, and money in response planning and application release management.

5.0 PURPLE TEAMS

Use of Purple Teams creates a formal link between Red and Blue Teams, as well as between Red Teams and application developers. Because time is of essence when managing the impact of a potential cyber incident, a shift toward proactive collaboration and continuous training is a must. There are several key approaches that Purple Teams can employ – to include tabletop exercises, side-by-side simulations, and use of preemptive cyber defense solutions. Purple Teams further align with and support the movement toward automated, moving, targeted defense (AMTD). Each of the above strategies are described in more detail below.

Having seasoned Red Team experts running tabletop exercises and scenario-planning exercises on historical cyber events (e.g., TTPs) provides a valuable starting point when used to help understand potential disruption points, business impacts and the actions / remediations to reduce those impacts and facilitate continued operations. Tabletop exercises represent a fundamental first step in building capability and confidence because the test the effectiveness of existing cybersecurity policies, procedures, and technologies. It helps identify gaps in policies, such as unclear roles or outdated protocols, and provides the opportunity to improve or create new ones. Cyber table-top exercises further allow organizations to prepare for different types of cyberattacks, from ransomware to insider threats or distributed denial-of-service (DDoS) attacks. This gives organizations a better understanding of how various threats would impact their operations, and the types of responses and mitigations that are needed. For example, these documented results can be used to create more tailored playbooks for Blue Teams.

Cyber simulations replicate the environment of a real cyberattack, or adversarial TTPs. By practicing decision-making in such scenarios, the leadership and cybersecurity teams can learn to make better, faster, and more informed decisions before an attack occurs. This is most evident when it comes to securing applications or network configurations. Purple Teams can simulate the potential impact of existing or new vulnerabilities to see potential impacts in a test or safe environment. This way, an organization can achieve greater assurance that an application will not be immediately compromised when it is fully implemented and released. By continuing to test and train, the Purple Teams can be used to create a structure and to build workflows that promote collaboration throughout the organization (and key stakeholders), thereby improving remediation efforts and optimizing security investments.

An integral component of Purple Teams is researching and helping organizations adopt preemptive cyber defense solutions – solutions are typically designed to be integrated with existing detection and response technology solutions, rather than being used as separate, stand-alone solutions. These technologies use additional software-based agents, decoys, and other sensors to add their own unique detection capabilities to continuously monitor and analyze activity within an environment and more rapidly identify any unusual, unexpected or potentially malicious activity. In these solutions, anomalies

trigger automation that moves beyond basic blocking and process termination. This includes deception, isolation, blocking access, modifying security controls in near real time, executing automated predefined or AI-generated security playbooks, or taking systems offline.

By leveraging preemptive tools and processes, organizations can quickly uncover, visualize, and/or respond to cyberattacks without relying on human intervention. Preemptive cyber defense is an essential component of any organization’s cybersecurity strategy and aligns with the implementation of Automated Moving Target Defense (AMTD) technology. AMTD involves moving, changing, obfuscating, or morphing attack surfaces to disrupt adversaries’ cyber kill chain.

AMTD technologies offer a new way to address threats with a preemptive cyber defense strategy, rather than focusing on traditional reactive methods of detection and response. It incorporates the use of software-defined architectures, polymorphism (in some cases), and the ability to dynamically change various components within the IT environment to confuse and disrupt potential attackers. This is especially important when it comes to disrupting emerging, AI-enabled attackers because it creates an unexpected amount of randomization and obfuscation that further complicates or blocks the potential attack vectors that threat actors are most likely to use. Purple Team ownership [of AMTD approaches] is critical as it helps integrate multiple components (e.g., Blue Teams, Red Teams, business owners, and application developers) across organizations.

6.0 APPLICATION DEVELOPMENT TEAMS

Application Developers are experiencing more pressure than anytime previously to improve the security of applications without disrupting flow or hindering innovation. The reality of improving security in software engineering is a multi-faceted, multi-year program that requires cooperation from numerous stakeholders, to include software engineers, Blue Team, Red Team, Purple Team, operations, and architecture teams.

Security in DevOps (DevSecOps) is a top issue for application developers. According to the *Software Engineering Survey for 2024*, lack of application security skills is considered a pain point by close to two-thirds of software engineering leaders.ⁱⁱⁱ The challenge of balancing software stakeholder concerns and business goals with security is consistently a challenge. This is where Purple Team and application developer integration through the adoption of a DevSecOps Model will help guide software engineering leaders to find the appropriate balance. This balance can be summarized in the following areas:

- **Security Knowledge, Skills, and Abilities** – Improving security skills and knowledge for software engineering improves security outcomes. By having Purple Teams provide security-focused training, it promotes more focused learning and engagement, while resulting in higher levels of knowledge retention.
- **Developer Enablement** – Core to developer enablement is reducing dependencies on external teams. When software engineering staff are more directly involved in activities traditionally owned by cybersecurity, there are better security outcomes. Being directly involved does not necessarily mean that software engineering owns all security concerns. Direct collaboration with security Purple Teams helps prop up software engineers to conduct work on their value stream with little direct dependencies acting as a constraint.

- **Secure Design and Threat Assessment** – Software engineering is based on the concept of patterns. However software is sliced, there is a pattern solving problems and delivering value. Hence, there also exists anti-patterns in software. These anti-patterns can result in innocuous bugs or devastating security vulnerabilities. “Secure by Design” principles are more important than ever, which should be continuously communicated by Purple Team members. Secure-by-design examples include:
 - Establishing internal security controls.
 - Publishing high-level threat models.
 - Publishing detailed secure software development lifecycle (SDLC) self-attestations.
 - Embracing vulnerability transparency.
 - Using and publicizing well-known design patterns for secure coding
- **Automated Security Practices** -- Gartner survey results for security in software engineering show a 15% improvement in security outcomes when more security activities are automated.^{iv} Using automated scanning tools can easily identify known IT and software vulnerabilities.
- **Software Supply Chain Security** -- When broken apart, most code in software originates from third parties, primarily open-source. Attacks against the software supply chain are driving increasingly higher annual costs, so more attention is required for security in SDLC processes and tools. This understanding can come through more engagement between developers and the Purple Team.

Overall, consistent engagement with Purple Teams, and Purple Team-led Training is critical to the success of application developers and the business owners that they support. Fully integrating security understanding into the SDLC is essential and embedding the Purple Team as a connection point is a must.

7.0 The Solution Provider

Mission Multiplier is a certified small business headquartered in Huntsville, Alabama that specializes in full spectrum cybersecurity solutions – with a focus on cyber services for government and commercial markets, as well as the development of innovative tools and technologies. We are considered experts in the areas of Red, Blue, and Purple Teams; as well as DevSecOps and secure development. Mission Multiplier is one of a few organizations that has developed and implemented a robust Purple Team capability supporting a major United States government program.

Mission Multiplier was founded on a truly innovative business value proposition. For every hour a Mission Multiplier employee works, we direct a portion of the company profit to a local charity of the employee’s choice. In this way, each employee knows that not only are they getting to develop and deliver innovative cybersecurity services, but that they are directly giving back to the local community. Building on this principle, our goal is to multiply the successes that our clients achieve against their respective missions, while simultaneously enabling the missions of our employees – with the result of securing and enriching the communities we serve.

Mission Multiplier
1300 Meridian St N Suite 101 Huntsville, AL 35801
www.missionmultiplier.com



ⁱ [New survey reveals \\$2 trillion market opportunity for cybersecurity technology and service providers | McKinsey](#)

ⁱⁱ [Internet of Things and data placement | Edge to Core and the Internet of Things | Dell Technologies Info Hub](#)

ⁱⁱⁱ [Gartner Software Engineering Survey for 2024](#)

^{iv} [Trends to Guide Security Automation Decisions in Software Engineering](#)