The Summit Awaits...

Are you ready for the Purple Ascent?

Presented by
Ben Struebing

linkedin.com/in/ben-struebing/ ben.struebing@CyberNEX.io www.CyberNEX.io

September 2024

OVERVIEW

01

Importance of Purple Teaming

What is Purple Teaming and how it can help your team build a resilient ecosystem

02

Building a Purple Team Program

Core components of establishing a Purple Team program using the Purple Ascent Framework

03

Start Your Journey

Learn about various resources available to begin purple teaming

Purple teaming is more than defense —
it's about building a proactive, battle-ready team to tackle tomorrow's threats today.

TODAY’S CHALLENGES

- Organizations face a **constant battle** against **evolving threats** in a **dynamic digital world**.
- To **thrive in today's** dynamic market, it's **not enough** to merely **keep pace** with the **evolving threatscape**

Malicious actors constantly adapt and innovate their tactics

- Failure to anticipate and counter these advanced tactics can lead to catastrophic breaches, data loss, and/or reputation impacts.

Increasing complexity of interconnected systems

- The complexity of these environments demands a robust and adaptive security strategy to prevent potential vulnerabilities from being exploited.

Shortage of skilled and experienced personnel

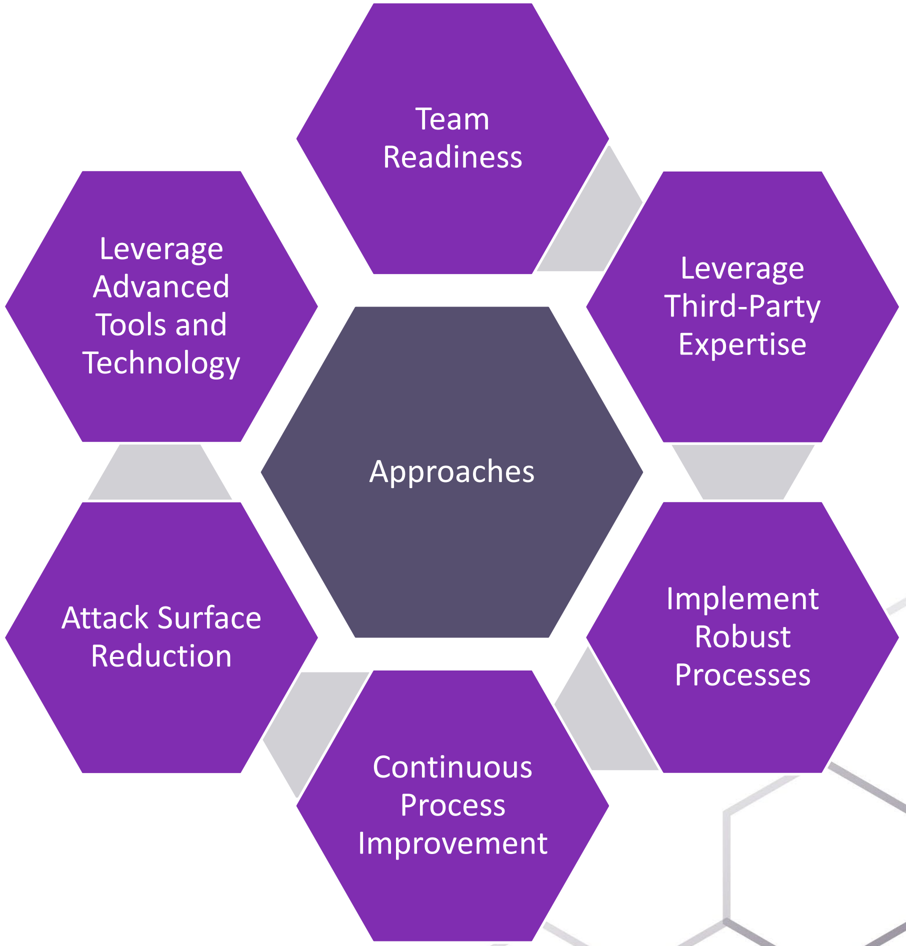
- Without skilled personnel, even the most advanced security technologies cannot be effectively utilized, leaving organizations vulnerable to attacks.

Doing More with Less

Strategies for Achieving Cyber Resilience

Business Objective

1. **Minimize impact on operations:** Cyber incidents cost businesses an average of $4.45M/breach in 2023
2. **Optimize the utilization of existing resources**: Effective resource utilization can reduce the time to detect and respond to threats by up to 50%
3. **Eliminate redundant or unnecessary assets**: 30% of IT budgets are spent on redundant or underutilized assets


Team Readiness
Leverage Advanced Tools and Technology
Leverage Third-Party Expertise
Approaches
Attack Surface Reduction
Implement Robust Processes
Continuous Process Improvement

Purple Teaming

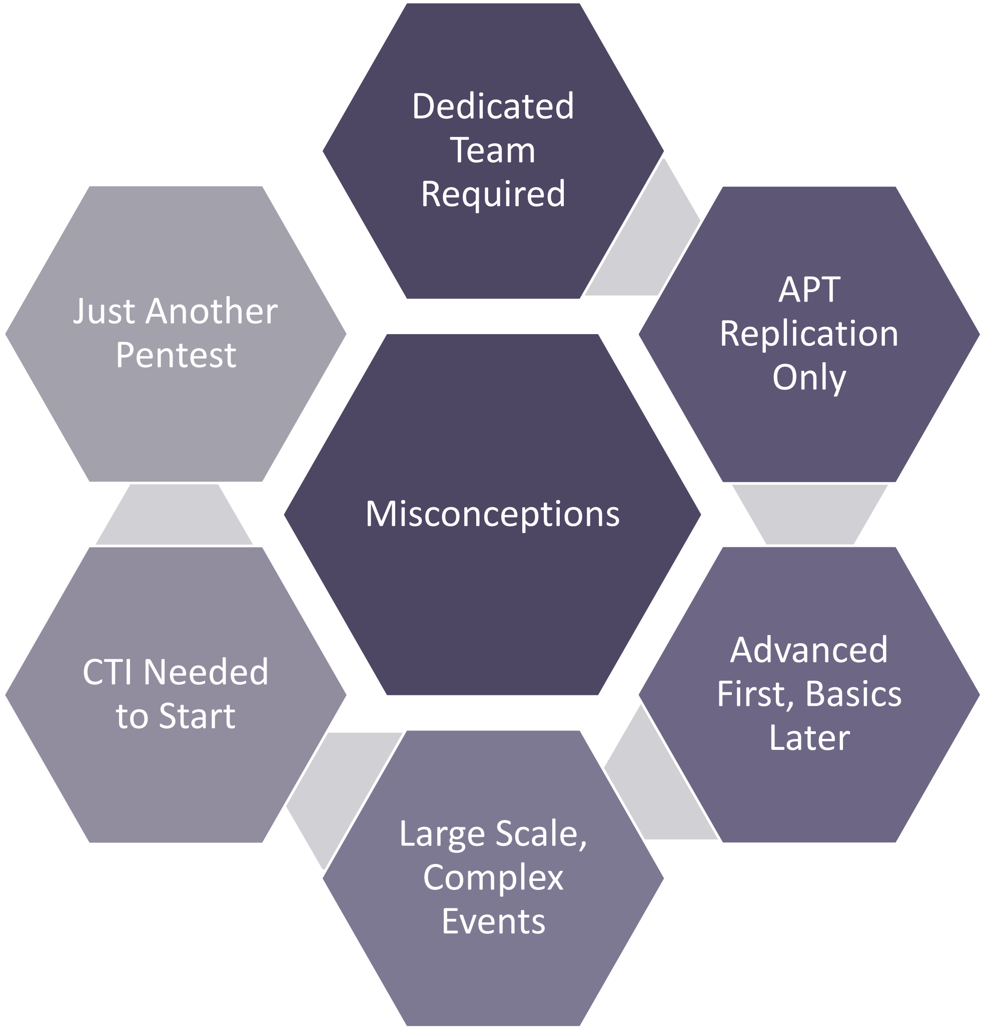
A Proactive Approach to Cybersecurity

Purple teaming is a **collaborative, continuous process** where offensive (red) and defensive (blue) teams work together to test and improve an organization’s cybersecurity defenses through **realistic threat simulations** and an emphasis on learning and adapting.

- Collaboration Across Teams
- Continuous Learning
- Realistic and Relevant Threat Simulations
- Proactive Mindset
- Holistic Approach
- Transparency & Empowerment

Purple Teaming

Common Misconceptions



Purple teaming can sometimes feel complex or out of reach, especially for smaller teams.

But many common misconceptions create unnecessary barriers.

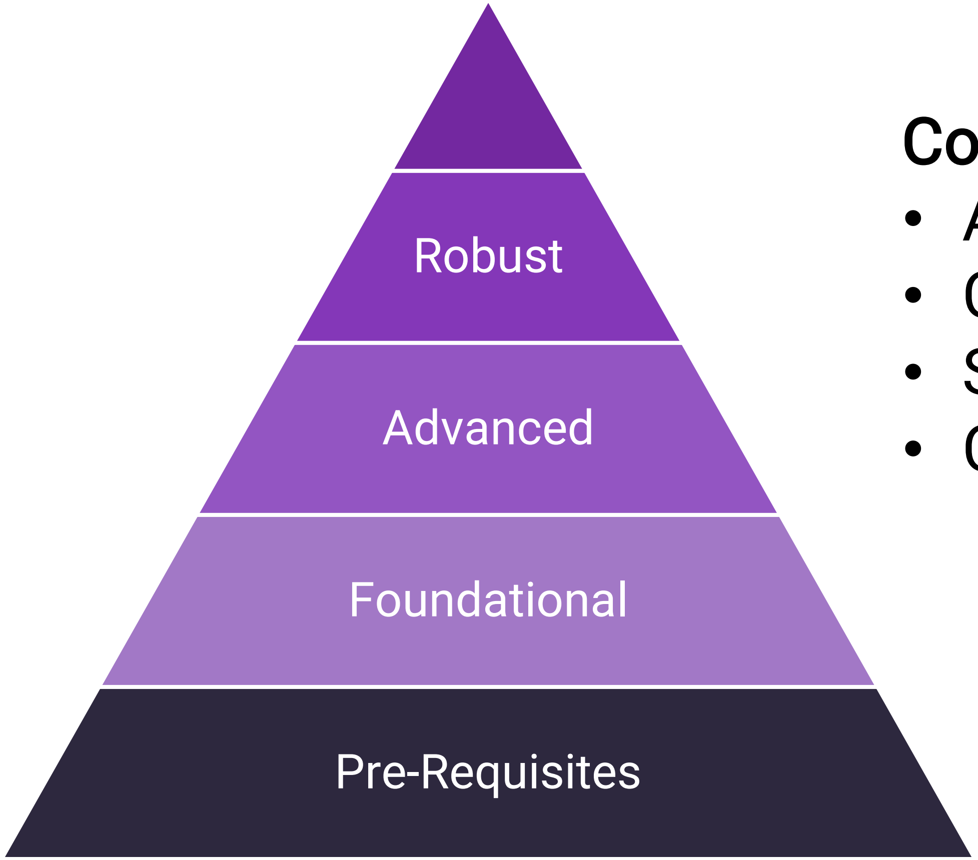
Let’s debunk these myths to make purple teaming accessible and effective for teams of any size.

The Purple Ascent

Framework

Definition

The Purple Ascent Framework



A structured roadmap designed to guide organizations on their **purple teaming journey**

Core Elements:

- A Clear Roadmap for Starting Small
- Crawl, Walk, Run Approach
- Scalability and Flexibility
- Controlled Chaos

Pre-Requisites

The Purple Ascent Framework

Know Your Environment

- Inventory Assets
- Know Your Attack Surface
- Network diagrams

Cybersecurity Basics

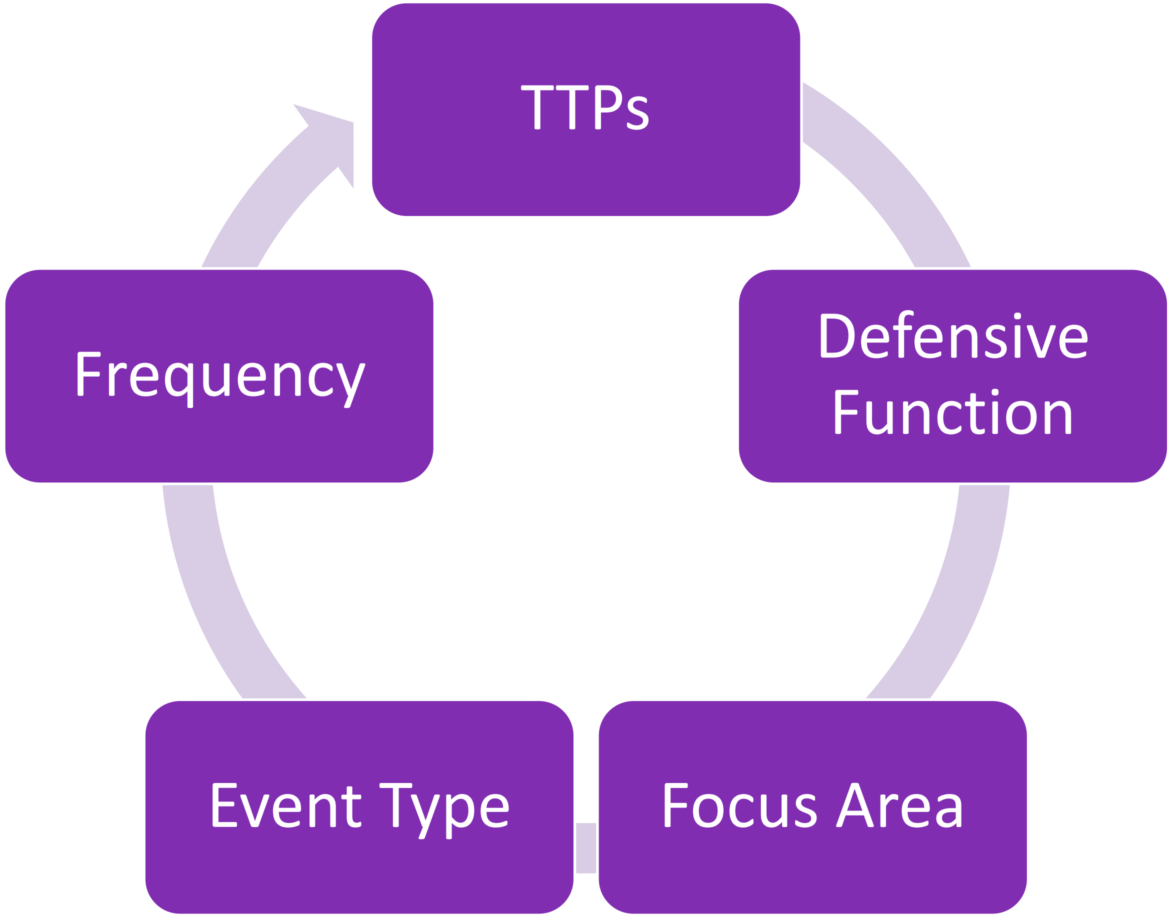
- Secure Network Design
- Controlled Use of Admin Privileges
- Secure Configuration for Hardware and Software
- Malware Defenses

Observability

- Monitor & Logging Capabilities

Key Factors

The Purple Ascent Framework



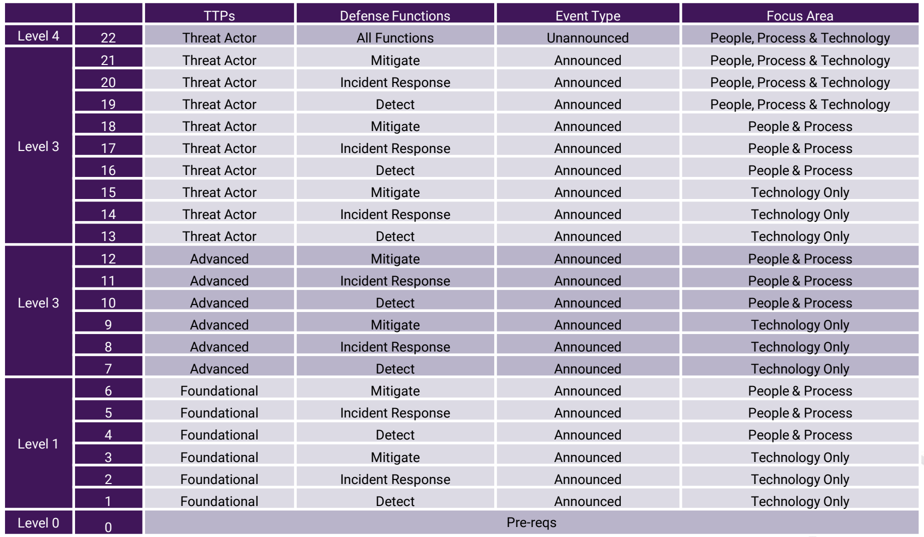
TTPs

Defensive Function

Focus Area

Event Type

Frequency



		TTPs	Defense Functions	Event Type	Focus Area
Level 4	22	Threat Actor	All Functions	Unannounced	People, Process & Technology
Level 3	21	Threat Actor	Mitigate	Announced	People, Process & Technology
	20	Threat Actor	Incident Response	Announced	People, Process & Technology
	19	Threat Actor	Detect	Announced	People, Process & Technology
	18	Threat Actor	Mitigate	Announced	People & Process
	17	Threat Actor	Incident Response	Announced	People & Process
	16	Threat Actor	Detect	Announced	People & Process
	15	Threat Actor	Mitigate	Announced	Technology Only
	14	Threat Actor	Incident Response	Announced	Technology Only
	13	Threat Actor	Detect	Announced	Technology Only
Level 3	12	Advanced	Mitigate	Announced	People & Process
	11	Advanced	Incident Response	Announced	People & Process
	10	Advanced	Detect	Announced	People & Process
	9	Advanced	Mitigate	Announced	Technology Only
	8	Advanced	Incident Response	Announced	Technology Only
	7	Advanced	Detect	Announced	Technology Only
Level 1	6	Foundational	Mitigate	Announced	People & Process
	5	Foundational	Incident Response	Announced	People & Process
	4	Foundational	Detect	Announced	People & Process
	3	Foundational	Mitigate	Announced	Technology Only
	2	Foundational	Incident Response	Announced	Technology Only
	1	Foundational	Detect	Announced	Technology Only
Level 0	0	Pre-reqs			

Tactics, Techniques & Procedures (TTPs)

Design Your Objective

Master the Basics

Foundational TTPs

Uncover the Fundamental Tactics to Strengthen Your Cyber Defense.

Elevate Your Defense

Advanced TTPs

Delve into Advanced MITRE ATT&CK Techniques to Stay Ahead of Sophisticated Threats.

Unmasking the Shadows

Threat Actor TTPs

Arm your organization with the knowledge to detect, analyze, and thwart even the most elusive cyber adversaries.

Defense Functions

Design Your Objective

Detection Engineering Focus

Detect

A specialized **emphasis** on refining our **detection** capabilities. It encompasses the tools, methodologies, and expertise required to engineer robust and precise detection mechanisms.

Incident Response

Respond

A coordinated approach to managing and mitigating security incidents. It ensures we can swiftly **identify**, **contain**, and **recover** from threats, minimizing potential damage and downtime while safeguarding our digital assets.

Mitigate for Resilience

Mitigate

A range of strategies, controls, and countermeasures designed to minimize vulnerabilities and **reduce the impact** of potential incidents.

Focus Areas

Design Your Objective

Technology Only	Evaluates an organization's IT **systems, hardware, software, and networks** to identify vulnerabilities and enhance cybersecurity defenses.
People & Processes	Focuses on an organization's **human resources** (i.e., training, experience) and **operational procedures** (including communication plan and roles & responsibilities)
People, Process & Technology	**A holistic evaluation** encompassing personnel, operational procedures, and technological infrastructure to enhance overall cybersecurity readiness and resilience.

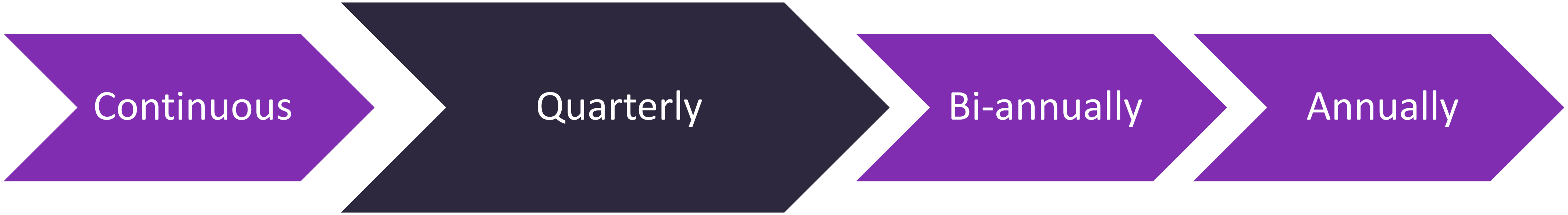
Event Type

Design Your Objective

Announced	Unannounced
• Focused on improving & learning • Team is focused, excited and has the right mindset for learning • Dedicated time period for learning • Execute more meaningful training events in a shorter time period • Controllable/tailored learning • Ramp up or slow down based on team's performance	• Focused on assessing the org • Team is living their daily routine • Occurs at random intervals • Execute most likely threats

Frequency

Design Your Objective



Continuous

Quarterly

Bi-annually

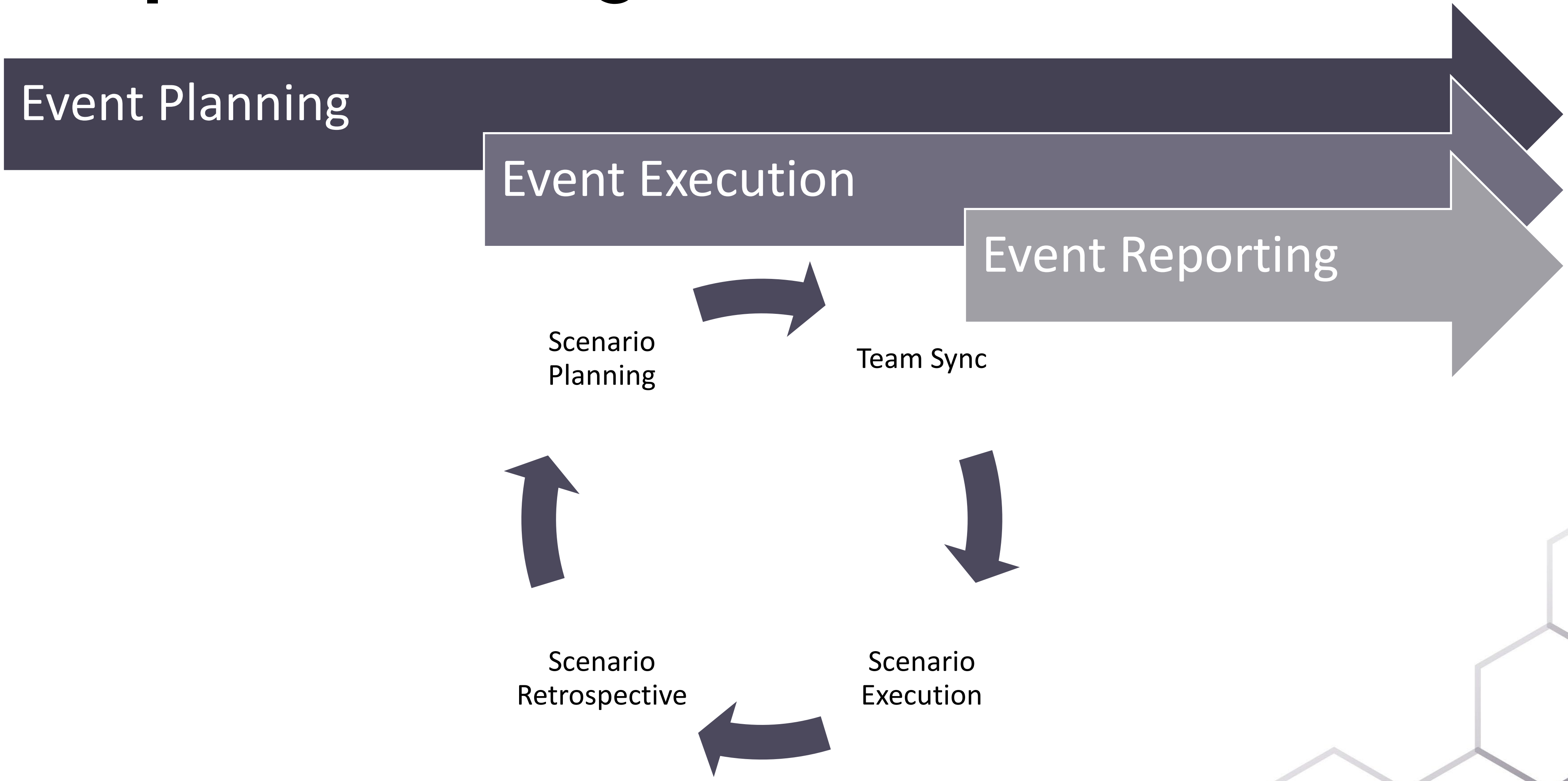
Annually

Purple Team

Event Management

From Vision to Victory

Purple Teaming Event



Event Planning

Event Execution

Event Reporting

Scenario Planning

Team Sync

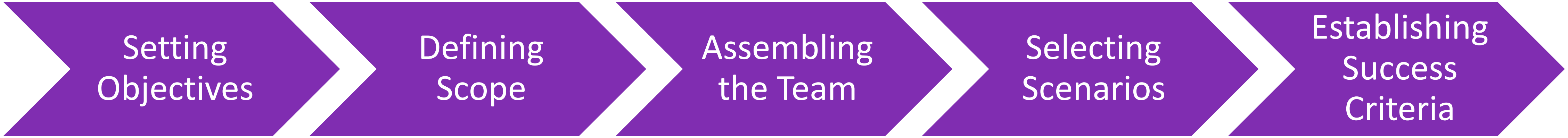
Scenario Execution

Scenario Retrospective

CyberNEX Technology

Planning

Purple Teaming Event



Setting Objectives

Defining Scope

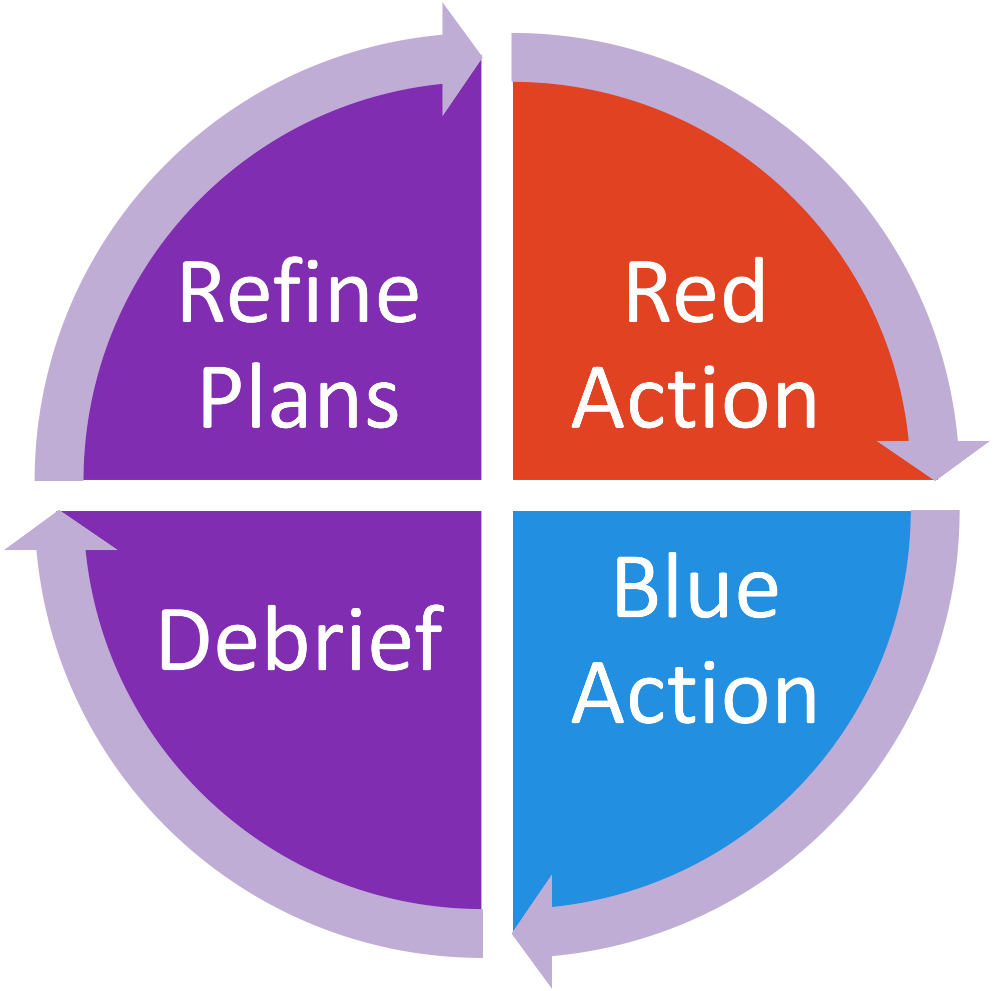
Assembling the Team

Selecting Scenarios

Establishing Success Criteria

Execution

Purple Teaming Event



Planning: Each team (red, blue, white) plans their role in the scenario.

Briefing: Share the scenario and ensure all teams understand the objectives.

Execute: Run the exercise, focusing on capturing what was done, what worked, and what didn’t.

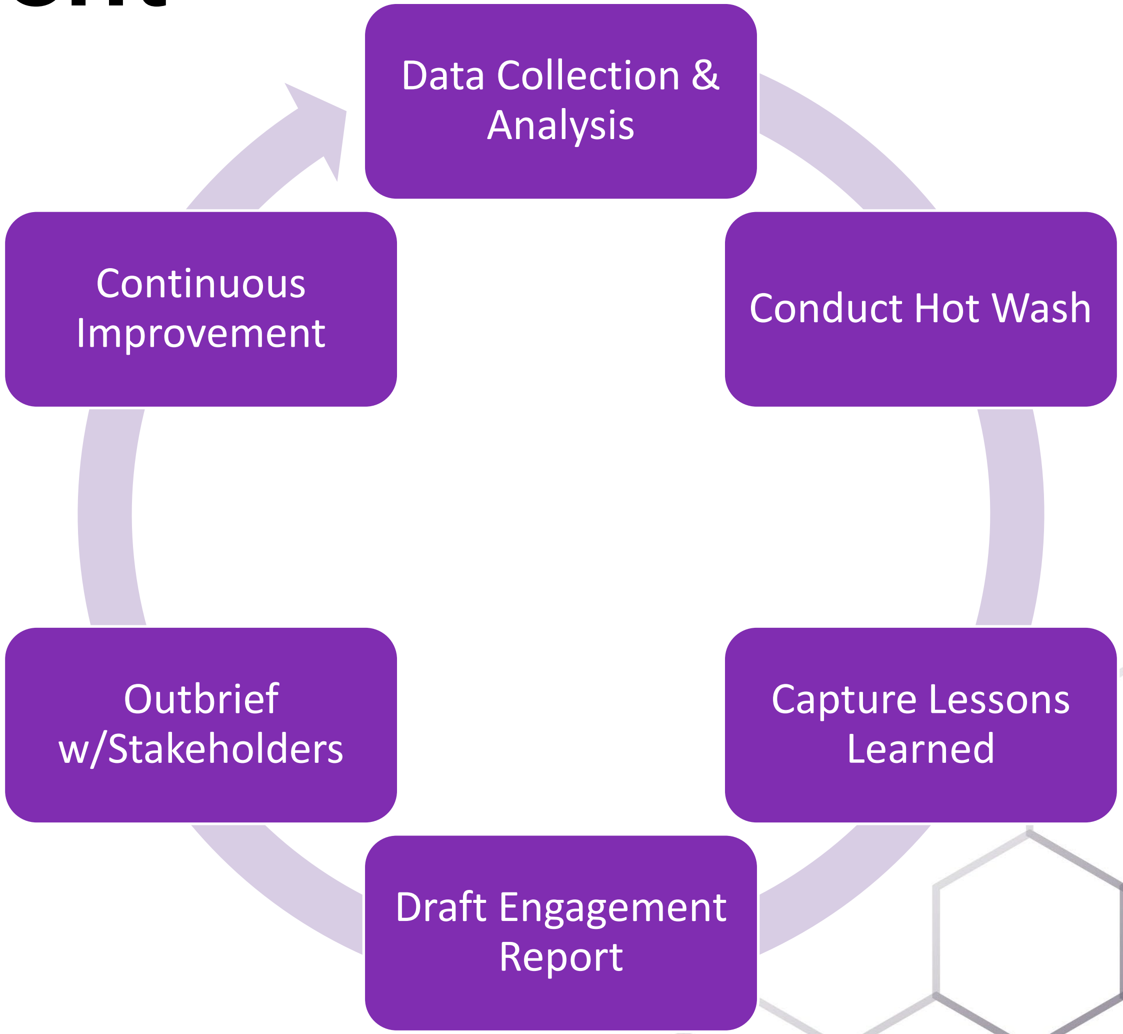
Debrief/Retrospective: Identify the major issues (big rocks), pinpoint root causes, and develop actionable lessons learned.

Refine Plans: Adjust tactics, defenses, and processes to address the gaps uncovered in the exercise, ensuring continuous improvement.

Reporting

Purple Teaming Event

Goal: Consolidate insights, enhances learning, drive improvements, inform stakeholders, and ensure compliance.


Data Collection & Analysis

Conduct Hot Wash

Capture Lessons Learned

Draft Engagement Report

Outbrief w/Stakeholders

Continuous Improvement

Purple Teaming

Next Steps

Available Resources

Do you want to know more?

Training

- SANS SEC599: Defeating Advanced Adversaries - Purple Team Tactics & Kill Chain Defenses
- Purple Teaming at GitLab
- HackTheBox – Enable Powerful Purple Team Security Ops

Articles

- CyberNEX - Latest Insights
- Scythe - Actionable Purple Teaming: Why and How You Can (and Should) Go Purple
- Splunk – The Purple Team: Combining Red & Blue Teaming for Cybersecurity

Frameworks

- The Purple Ascent
- Mitre ATT&CK
- Aerospace SPARTA
- Purple Team Exercise Framework (PTEF)

Tools

CYYNC BY CYBERNEX

PurpleOps

vectr

PlexTrac®

Summary of Key Points

Importance of a Progressive Approach to Purple Teaming

- Start with **basic exercises** and **gradually increase complexity** (crawl, walk, run).
- Ensure that each stage builds upon the previous one, enhancing team capabilities.

Structuring an Effective and Scalable Purple Team Program

- Define **clear goals and objectives** tailored to your organization's needs.
- Develop a structured plan with regular engagements and feedback loops.
- Incorporate a **mix of internal and external team members** for diverse perspectives.

Leveraging Available Resources to Get Started

- Utilize **existing tools and frameworks** (e.g., MITRE ATT&CK, Atomic Red Team, The Purple Ascent).
- Engage with professional training and service providers **to build expertise.**
- Foster a culture of **continuous learning and improvement** within the team.

The Summit Still Awaits

But now you’re ready for the Purple Ascent

Presented by
Ben Struebing

linkedin.com/in/ben-struebing/ ✉ ben.struebing@CyberNEX.io www.CyberNEX.io