A DAMOCLES COMPANY

WHITE PAPER

THE LARES PURPLE TEAM METHODOLOGY

OVERVIEW

Lares Purple Teaming strengthens threat detection and response by combining offensive and defensive strategies. Through real-time attacks and collaboration between offensive and defensive teams, it drives continuous learning, measurable improvements, and custom playbook development, helping organizations defend against evolving cyber threats.

ABOUT LARES

Lares is a security consulting firm that helps companies secure electronic, physical, intellectual, and financial assets through a unique blend of assessment, testing, and coaching since 2008.

For more information, visit lares.com, contact us at (720) 600-0329, or follow Lares on Twitter @Lares_.

www.lares.com

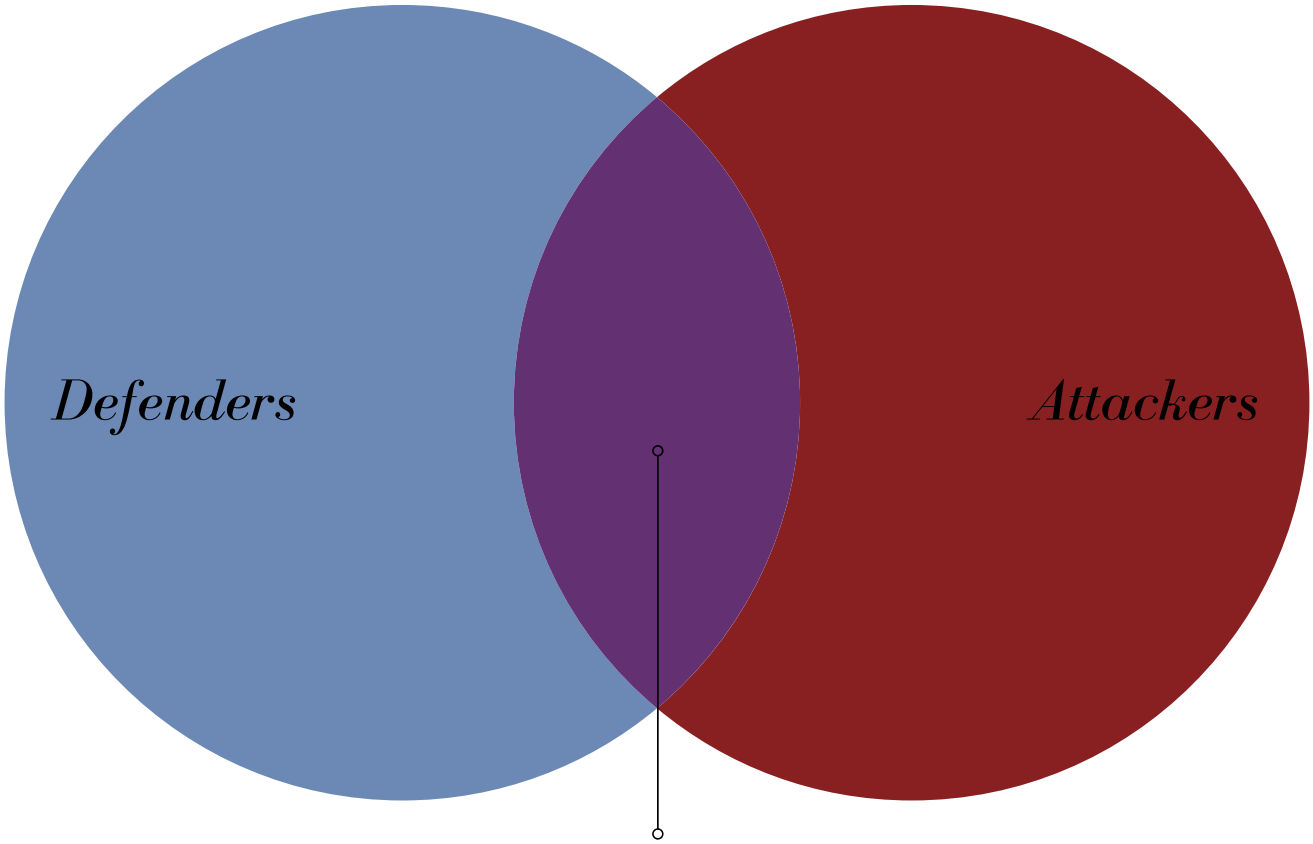
CONTACT INFORMATION

1580 N. Logan St. Ste 660, PMB 79199, Denver, CO 80203, USA

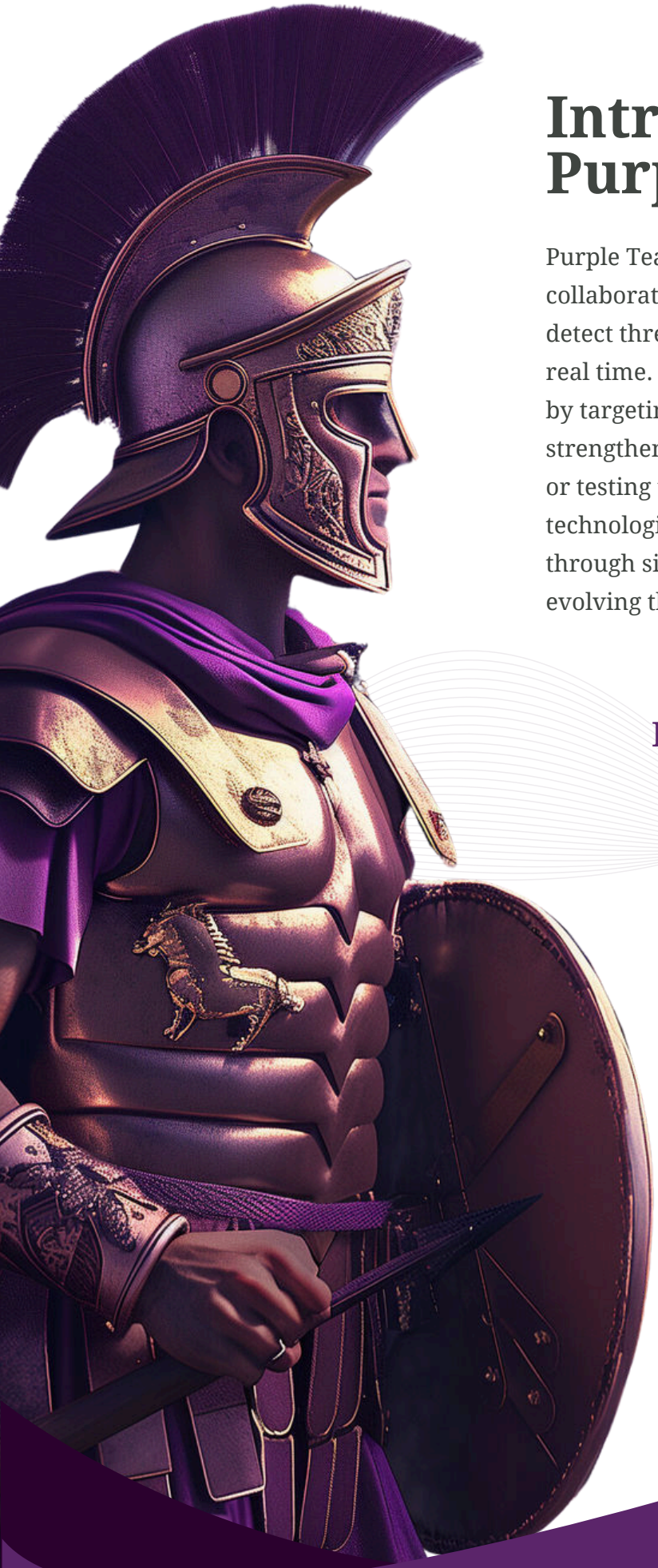
+1 (720) 600-0329
sales@lares.com

Executive Summary

Lares' Purple Teaming methodology blends offensive and defensive strategies to improve threat detection, response, and prevention. Organizations can address vulnerabilities and enhance defenses through measurable progress by leveraging real-time attack simulations and fostering continuous collaboration. Our methodology is focused on achieving client-specific goals and continuously improving people, processes, detections, and prevention mechanisms.



Defenders who learn from attackers



Introduction to Purple Teaming

Purple Teaming enables Red and Blue teams to collaborate dynamically, ensuring that organizations detect threats and learn and refine their defenses in real time. This method goes beyond penetration testing by targeting specific security objectives, whether strengthening incident response, improving telemetry, or testing the effectiveness of new detection technologies. Lares engineers actively guide your team through simulations to enhance preparedness against evolving threats.

Key Benefits of Purple Teaming

- **Hands-on Defense Improvement:** Interactive exercises that allow teams to learn how to respond to real-world threats.
- **Collaboration and Transparency:** Fosters an environment where offensive and defensive teams work together, increasing both teams' capabilities.
- **Measurable Progress:** Custom metrics track your organization's detection and response improvements over time.

Methodology Overview

Our Purple Team engagements are designed around **client goals**, focusing on improving specific security capabilities. The following phases ensure tailored and impactful exercises.

Phase 1: Scoping and Rules of Engagement

I

The engagement begins with the scoping of your organization's objectives. Key factors include:

- **Objective Setting:** Determine goals for the exercise, whether enhancing people, detections, improving incident response, or strengthening specific defenses.
- **Identifying Targets:** Selecting systems, networks, or cloud environments critical to your security.
- **Defining Engagement Boundaries:** Establishing clear Rules of Engagement (ROE) to ensure that business operations are not disrupted during testing.

Phase 2: Playbook Design and Objectives

II

This phase is about aligning the exercise with your organization's goals:

- **Tailored Playbook Development:** Lares collaborates with you to design attack scenarios—such as ransomware, kernel attacks, or EDR bypasses—customized to address your specific security gaps, whether improving detection rates or hardening critical systems.

Phase 3: Realistic Attack Simulations

III

Our adversarial engineers simulate sophisticated real-world attacks using a variety of tactics, techniques, and procedures (TTPs), including:

- **Advanced Persistent Threats (APTs)**
- **Ransomware Deployments**
- **Kernel Attacks**
- **EDR Bypass and Testing**

Lares engineers guide your team in **understanding attack behaviors** and **responding to the attacks in real time**, mirroring adversary tactics to train your team in recognizing and stopping them.

IV Phase 4: Defense Collaboration and Feedback

Lares engineers work side-by-side with your defensive teams to assess how well your defenses respond to simulated attacks:

- **Immediate Feedback:** Providing real-time insights to improve detection, incident response, and logging.
- **Custom Detection Rule Development:** We help your team create and refine detection rules based on gaps identified during simulations.
- **Tailored Playbook Adjustments:** As the engagement progresses, we fine-tune the playbook to ensure continuous improvement in addressing identified weaknesses.

V Phase 5: Measurement and Reporting

After the Purple Team exercise, Lares delivers comprehensive reporting with actionable insights:

- **Performance Metrics:** Time-to-detect, response accuracy, and success rates are tracked for each TTP.
- **Gap Analysis:** Detailed analysis of defensive gaps with recommendations for improving visibility, detection, and prevention.
- **Telemetry Review:** Insights into how well current systems (e.g., EDR, SIEM) capture and respond to simulated threats, with suggestions for enhancing telemetry and rule effectiveness.

VI Phase 6: Continuous Improvement and Learning

The end of the engagement is only the beginning. Continuous learning is at the heart of our Purple Team methodology:

- **Debrief Findings:** Reviewing key results and next steps in detail.
- **Refining Playbooks:** Custom playbooks are enhanced after each session based on the evolving threat landscape.
- **Ongoing Collaboration:** We ensure that your team stays updated on the latest TTPs and defensive strategies, promoting a culture of continuous learning.

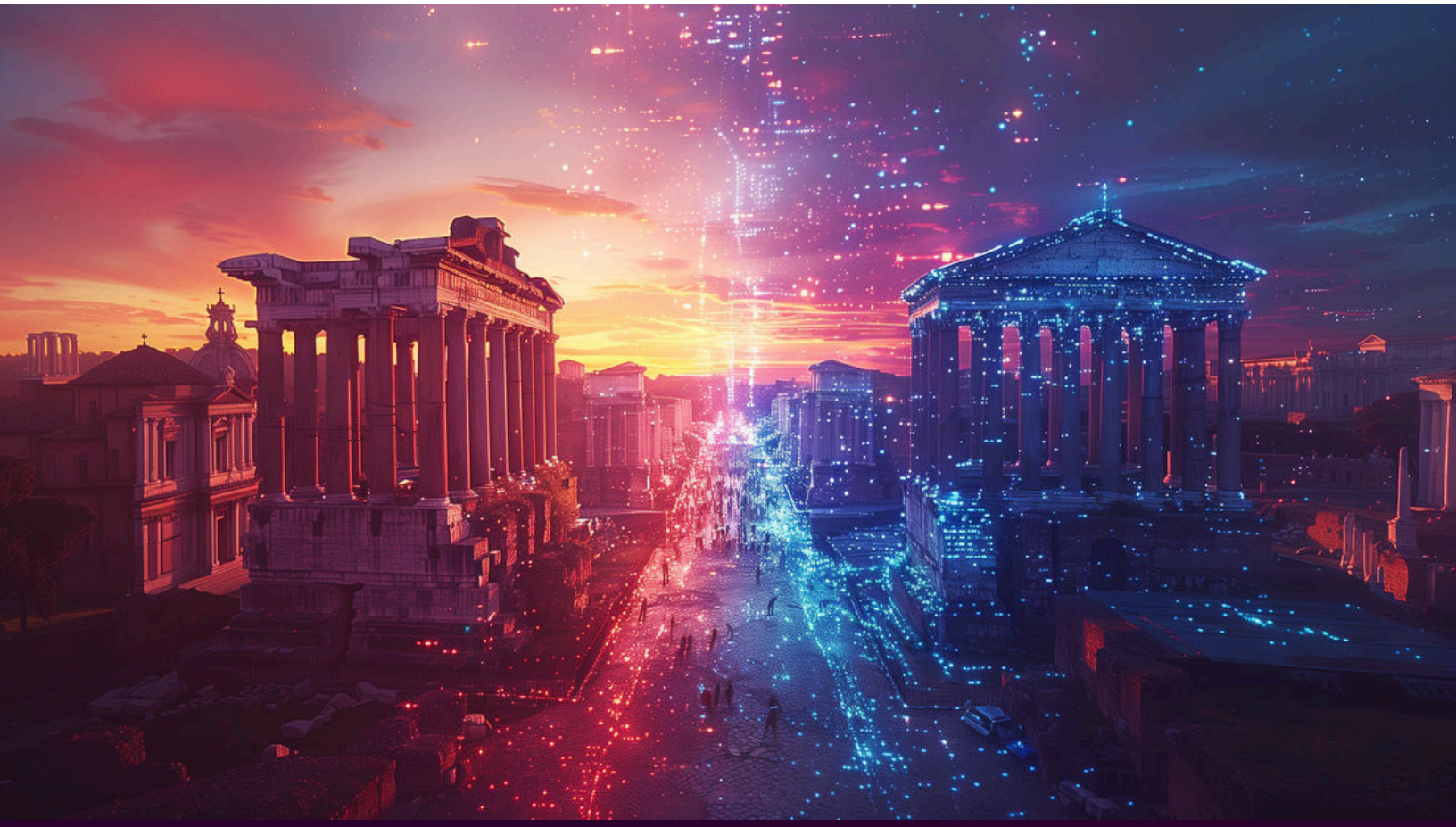
Key Deliverables

At the end of a Purple Team engagement, Lares provides comprehensive documentation and actionable guidance:

- **Executive Summary Report:** A tailored summary for senior management, highlighting high-level findings, gaps, and remediation steps.
- **Detailed TTP Catalog:** A breakdown of every attack scenario executed, including success and failure metrics.
- **Custom Playbooks:** Incident response and detection playbooks specific to your environment.
- **Ongoing Metrics Tracking:** Progress metrics aligned with frameworks like MITRE ATT&CK, demonstrating improvements over time.

Conclusion

Purple Teaming with Lares builds resilient organizations through active collaboration and continuous improvement. By simulating real-world attack scenarios, your team gains valuable experience while strengthening your security posture in real-time. **Transparency, measurable progress, and practical learning** are at the heart of every Lares Purple Team engagement, ensuring your defenses evolve to meet today's sophisticated threats.



ABOUT LARES

Lares is a security consulting firm that helps companies secure electronic, physical, intellectual, and financial assets through a unique blend of assessment, testing, and coaching since 2008.

For more information, visit lares.com, contact us at (720) 600-0329, or follow Lares on Twitter @Lares_.

LARES
A DAMOVO COMPANY

CONTACT INFORMATION

1580 N. Logan St. Ste 660, PMB 79199, Denver, CO 80203, USA

+1 (720) 600-0329
sales@lares.com