Business Perspective & Planning

Strategizing Controlled Attacks for Cyber Resilience

Topics: Objectives | Policy | Challenges | Planning | Logistics

UNDERSTANDING BUSINESS REQUIREMENTS

- → **Strategic Alignment:** Security initiatives must directly support organizational growth and business continuity.
- → **Risk Mitigation:** Proactive management of digital threats to protect physical and intellectual assets.
- → **Value Proposition:** Cybersecurity investments should yield measurable ROI in resilience and trust.
- → **Assessment:** Controlled attacks serve as the benchmark for organizational resilience against real-world threats.

GOVERNANCE & OBJECTIVES

Core Objectives

Protect critical assets, ensure service reliability, and achieve regulatory compliance while minimizing financial risks.

Security Policy

Establish high standards and procedures that define employee responsibilities and incident response frameworks.

Stakeholder Trust

Maintain customer and investor confidence through verified security practices and consistent policy enforcement.

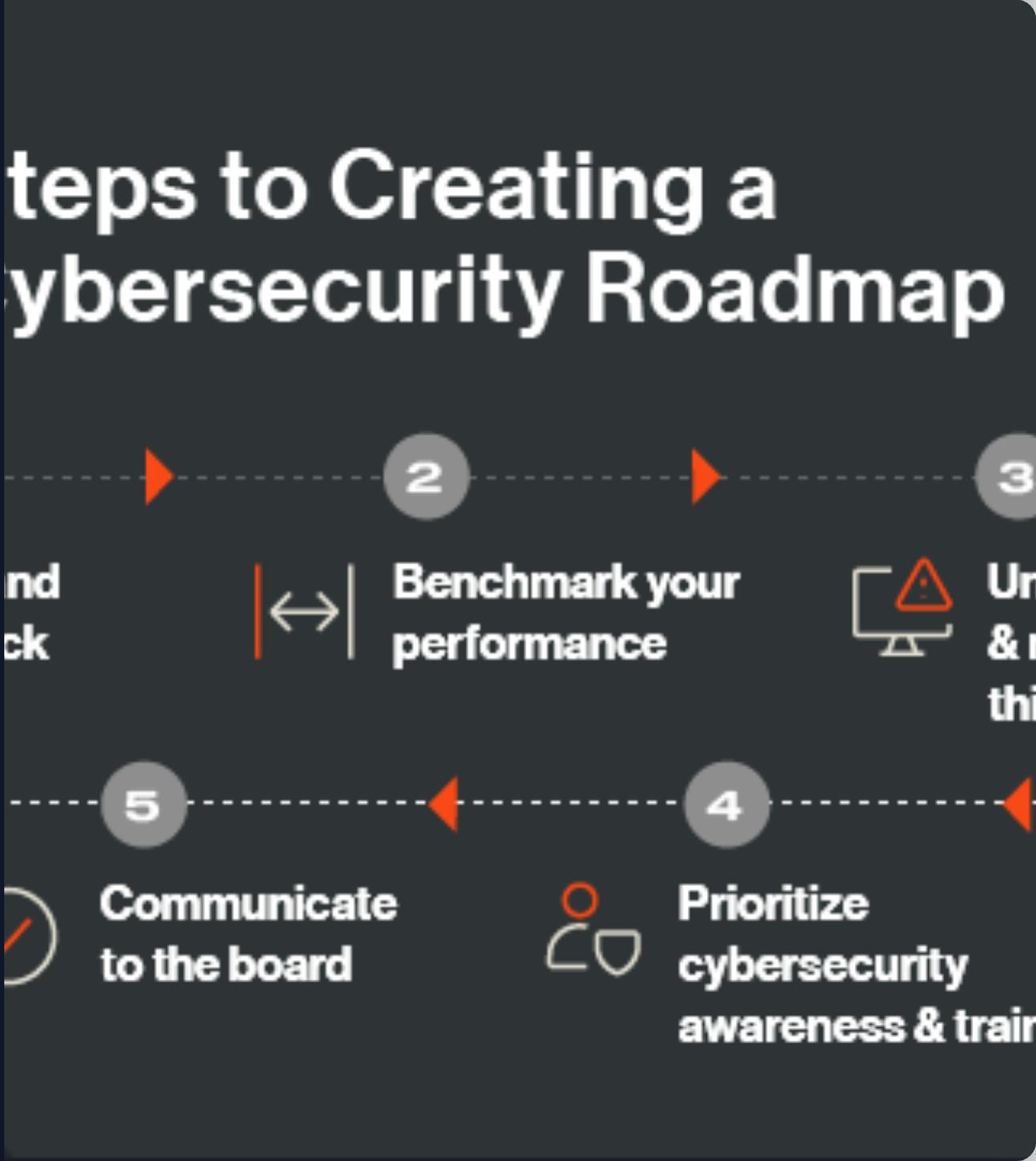
RESULTS VS. CHALLENGES

Historical Test Metrics	Current Business Challenges
• Penetration Testing Reports • Vulnerability Assessment Findings • Audit and Compliance Records	• Evolving Cyber Threat Landscape • Budget and Resource Constraints • Skills Shortage in Cybersecurity
• Incident Response History • Remediated vs. Accepted Risks	• Rapid Adoption of Emerging Tech • Stringent Global Privacy Regulations

STRATEGIC PLANNING

A controlled attack requires meticulous preparation to ensure safety and effectiveness.

- **Rules of Engagement (RoE):** Define boundaries and testing methodologies.
- **Asset Identification:** Pinpoint critical systems that require deep inspection.
- **Management Authorization:** Explicit written consent is non-negotiable.
- **Success Criteria:** Clearly defined KPIs for reporting.



CONSTRAINTS & TIMING

Inherent & Imposed Limitations

- → Limited testing duration and restricted system access.
- → Operational constraints preventing full-scale simulations.
- → Legal, regulatory, and budgetary boundaries.

Timing Strategy

Timing is everything. Schedule assessments during:

- → Off-peak operational hours to avoid service disruption.
- → Periods of low business activity.
- → Post-deployment phases of new infrastructure.

TECHNICAL PARAMETERS

Attack Types

Black Box: Zero Knowledge
Gray Box: Partial Knowledge
White Box: Full Knowledge

Source Points

Assessments originating from External Internet, Internal Intranet, or Cloud-based entry points.

Required Knowledge

Deep understanding of network architecture, OS, security controls, and specific business workflows.

ATTACK LIFECYCLE & TEAMING

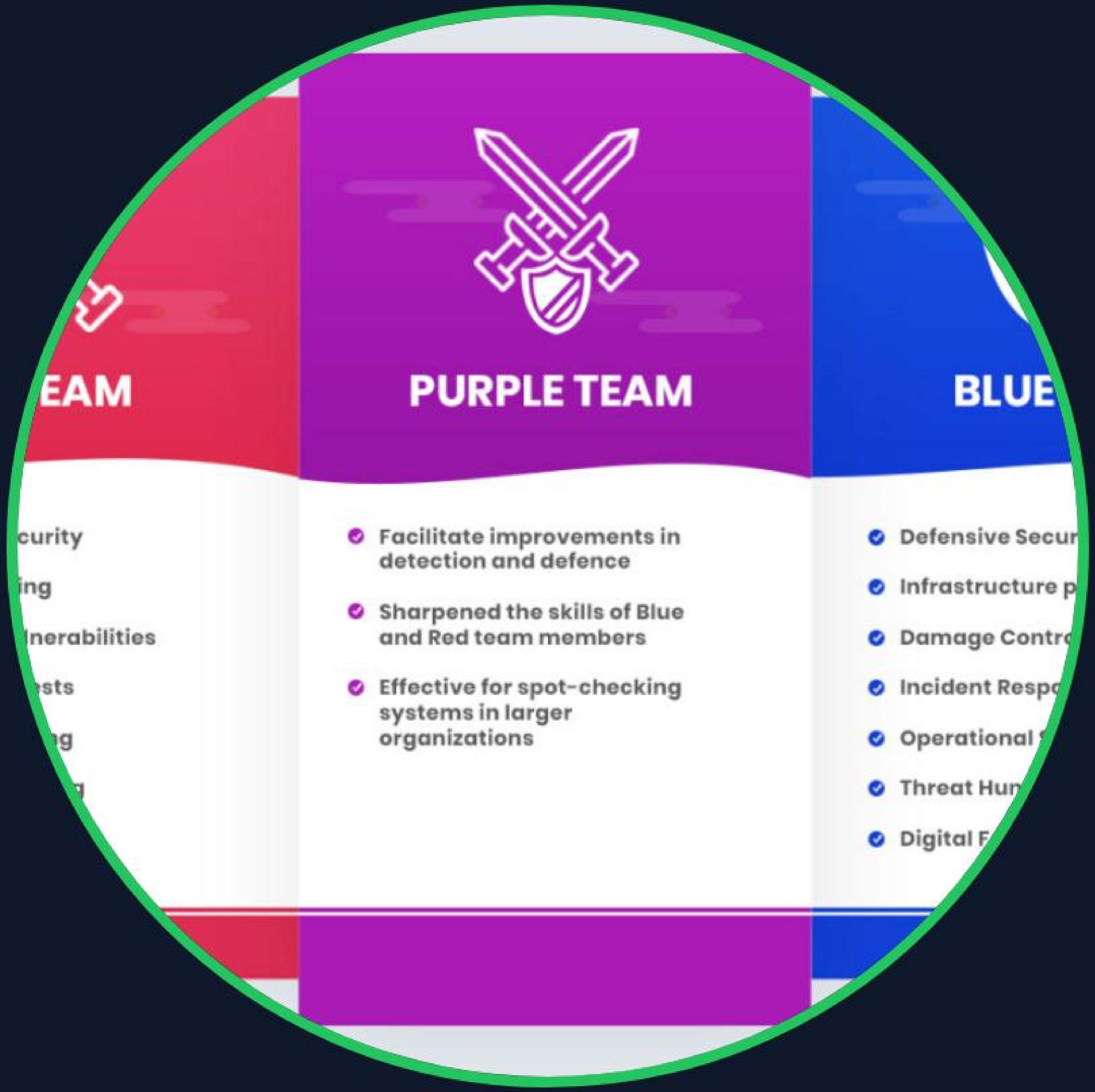
Recon	Scanning	Exploit	Privilege	Maintain	Report
Gathering Info	Finding Gaps	Gaining Access	Escalation	Post-Exploit	Analysis

RED TEAM
Attackers

BLUE TEAM
Defenders

PURPLE TEAM
Collaborators

ENGAGEMENT PERSONNEL



- → **The Planner:** Defines scope, coordinates resources, and manages communications.
- → **The Consultant:** Provides high-level technical expertise and remediation roadmaps.
- → **The Tester:** Executes the technical assessments and documents all technical findings.

Selection Criteria: Technical certifications, ethical conduct, and professional integrity.

LOGISTICS & LEGAL COMPLIANCE

Operational Logistics

Ensuring specialized tools, communication channels, and secure data handling procedures are in place.

Law Enforcement

Rigorous compliance with applicable cyber laws is mandatory. Maintain comprehensive evidence trails and coordinate with authorities for formal investigations when required.

IMAGE SOURCES

https://c5insight.com/wp-content/uploads/2025/06/white-paper-airplanes-offcourse-yellow-airplane-business-technology-strategy-alignment.jpg

Source: c5insight.com

https://www.bitsight.com/sites/default/files/2024/10/28/5%20Steps%20to%20Creating%20a%20Cybersecurity%20Roadmap.png

Source: www.bitsight.com

https://cyberhoot.com/wp-content/uploads/2022/03/Red-Purple-and-Blue-Team-Exercises-1000x700.jpg

Source: cyberhoot.com

Thumbnail for www.rev.com

https://cdn.prod.website-files.com/65e5ae1fb7482afd48d22155/68f78c1289807750b35576e0_Law%20Enforcement%20Technology%20Shaping%20the%20Future%20of%20Cases1.webp

Source: www.rev.com

https://connection-technologies.co.uk/wp-content/uploads/2026/05/best-cyber-security-companies-uk-2026.jpg

Source: connection-technologies.co.uk