



scythe.io



Red Team Operations Roadmap

A Practitioners Guide to Red Teaming

Author

Marc Brown

Contributors

Maril Vernon, Principal Application Security Architect, Aquia (2023 Woman Hacker of the Year)
Justin Elze, CTO, TrustedSec
Savannah Lazzara, Lead of Red Team Village
Tim Medin, CEO, Red Siege

Contents

Introduction

Why Red Teaming Is important

PHASE 1: Building the Foundation

PHASE 2: Operationalizing Your Program

PHASE 3: Elevating Program Efficacy

PHASE 4: Sustaining Your Program

Conclusion & Recommendations

References



Introduction

It's no secret that cyber threats are growing more sophisticated by the day; the role of offensive security operations has never been more critical. A Red Team, tasked with mimicking adversaries, plays a pivotal role in an organization's cybersecurity strategy. By emulating realistic cyber attacks, Red Teams provide invaluable insights into vulnerabilities and deficiencies in security defenses, offering a unique perspective essential for fortifying an organization's cyber resilience.

This eBook serves as a comprehensive roadmap for organizations at any stage of their Red Team maturity—whether you're initiating a Red Team program or seeking to elevate your existing operations. Our goal is to guide you through the journey of building a robust Red Team capability, operationalizing your strategies, elevating your practices to align with advanced threat landscapes, and sustaining your operations to continuously adapt to new challenges.

Why Red Teaming Is important

It's no secret that having an independent assessment of your security posture is critical today, leading to more investments in proactive security measures, including the creation of Red Teams. But why? And how should an organization go about the creation and advancement?

The primary value of creating or advancing a Red Team within an organization lies in its ability to provide a proactive and comprehensive assessment of the organization's security posture. By simulating sophisticated cyber attacks, the Red Team uncovers hidden vulnerabilities, tests the effectiveness of security controls, and challenges the assumptions of the Blue Team's defensive strategies. This process not only strengthens the organization's ability to detect and respond to real-world threats but also fosters a culture of continuous improvement and collaboration between the Red and Blue Teams. As a result, the organization becomes more resilient, agile, and capable of safeguarding its assets and reputation in an ever-evolving threat landscape.





PHASE 1

Building the Foundation

The journey begins with laying a solid foundation for your Red Team operations. This stage is about establishing the core elements that form the basis of effective Red Teaming, including defining your team's objectives, scope, and rules of engagement. Building the foundation also involves assembling a skilled team with diverse backgrounds to mimic various adversary tactics, techniques, and procedures (TTPs) effectively. The key aspect of this stage is developing a comprehensive understanding of your organization's digital environment and potential attack surfaces.

Here's a detailed approach to building a solid foundation for your Red Team operations.

Understand Your Organization's Objectives: The first step in establishing a successful Red Team is clearly understanding what you aim to achieve through these operations.

- a. **Define Goals and Scope:** Start by articulating the specific objectives of your Red Team operations. Whether identifying vulnerabilities, testing incident response capabilities or improving security awareness, having clear goals will guide your team's efforts and focus.
- b. **Align with Stakeholders:** Engage with key organizational stakeholders to gather insights on their security concerns, expectations, and desired outcomes from Red Team activities. This alignment ensures that Red Team operations are relevant and contribute value to the broader organizational objectives.

Build Capability: Assembling a team with the right mix of skills and ensuring they have the necessary resources is crucial for the success of Red Team operations.

- a. **Assemble a Dedicated Red Team:** Recruit individuals with diverse skill sets, including penetration testing, cyber threat intelligence, software development, and social engineering, to cover a wide range of attack vectors and methodologies.
- b. **Ensure Access to Resources:** Equip your Red Team with the necessary hardware, software, and access to training resources. This includes specialized penetration testing tools, secure testing environments, and ongoing professional development opportunities to stay abreast of the latest attack techniques and defense strategies. Even more critical is giving the team time and the flexibility needed to be responsive and agile. Teams need time to understand, integrate, and train while building new capabilities. Contrary to many IT policies, teams also need flexibility and be empowered to spin up cloud resources as needed. Today's policies are quite restrictive, usually taking CISO/CTO buy-in and the ability to use a Pcard or something outside the regular IT purchasing routes.

Establish Rules of Engagement (ROE): Defining what is and isn't within the scope of Red Team operations is vital to ensure the safety and integrity of organizational assets during testing.

- a. **Define Scope and Limits:** Clearly outline the boundaries of Red Team activities, specifying what systems, data, and methods are off-limits to avoid unintended disruption or exposure of sensitive information. For safety-critical or mission-critical systems, such as OT/ICS and medical devices, Red Teams should employ techniques like threat modeling, architecture reviews, and static analysis or leverage maintenance cycles to assess vulnerabilities and risks to minimize disruption concerns.
- b. **Document and Communicate Success KPIs:** Establish key performance indicators (KPIs), discussed below, that reflect the objectives of Red Team operations. Share these KPIs with stakeholders and the defensive security teams to provide a clear benchmark for measuring success and impact.
- c. **Identify Trusted Agents & Key Stakeholders:** Understanding who is involved with any Red Team operations is critical. Being able to identify and effectively communicate with stakeholders from different sections of your organization is a must. Even more important, give your team time! Time to research, understand, integrate, and train while documenting new capabilities. Equally important, limit your trusted agents (maybe to 2 and no more), focusing your team. Having too many individuals involved could jeopardize the engagement.

Documentation and Reporting: Maintaining detailed records of Red Team tactics, techniques, procedures (TTPs), and findings is crucial for tracking progress, sharing knowledge, and informing future security improvements.

- a. **Develop a Standardized Methodology:** Create a framework for how testing is planned, executed, and reported. This standardization ensures consistency in testing and allows for accumulating comparable data over time. This could include: frameworks, Gant chart templates, and report samples.
- b. **Create a TTP Repository:** Develop a centralized repository for documenting all used TTPs, as well as any identified vulnerabilities, exploits, and remediation strategies. This resource serves as a valuable knowledge base for both current and future Red Team members and aids in the continuous refinement of your organization's cybersecurity defenses.
- c. **Provide Feedback and Communications:** Provide feedback to the Red Team from any engagements run so they can also improve capabilities. Ensure all stakeholders are in the loop and agree on reporting procedures.

By carefully building the foundation of your Red Team operations, you lay the groundwork for a proactive, strategic approach to identifying and mitigating cybersecurity risks. This foundational phase not only sets the stage for more advanced Red Teaming activities but also ensures that your efforts are aligned with your organization's broader objectives and risk management strategies.



PHASE 2

Operationalizing Your Program

Once the foundation is laid, the next step is to operationalize your Red Team operations. This stage focuses on integrating Red Teaming into the broader cybersecurity strategy of your organization. It involves regular and systematic simulation exercises, developing a streamlined process for planning, executing, analyzing, and reporting on Red Team engagements. Operationalizing your Red Team efforts ensures that findings and insights translate into actionable intelligence, leading to tangible improvements in your cybersecurity posture.

Operationalizing Red Team operations is a critical step in enhancing an organization's cybersecurity defense mechanisms. This phase involves a strategic approach to tool selection, threat emulation, scenario-based testing, and collaboration with defensive security teams. Here's how organizations can deepen their operational capabilities to ensure that Red Team efforts are not just exercises but integral parts of a holistic security strategy.

Tool Selection and Enhancement: The effectiveness of Red Team operations significantly depends on the tools and technologies at their disposal. Selecting and enhancing the right tools is not just about replicating adversarial tactics but doing so in an efficient and scalable manner. Allocate time and resources to choose the tools necessary, as tooling will provide team members with foundational support.

- a. **Identify and Implement Emulation Tools:** Choose tools that can emulate a wide range of real-world threats, such as Breach and Attack Simulation (BAS) tools like SCYTHE, AttackIQ, Picus, or others. These tools should allow Red Teams to simulate sophisticated cyber-attack scenarios across various vectors, including email, web, and endpoint.
- b. **Implement BAS+ Platforms for Continuous Testing:** Advanced platforms enable one-off testing and continuous security assessments and improvements. These platforms should facilitate ongoing testing, providing real-time insights into vulnerabilities and the effectiveness of current security measures.
- c. **Evaluate Attack Impact:** Use these tools to understand whether an attack can be successful and the potential impact on the organization's security posture. This involves mapping out potential breach paths and identifying critical assets at risk.

Emulate Real Threats: Mimicking real-world threats involves deeply understanding the current threat landscape and adapting quickly as new threats emerge.

- a. **Research and Replicate Latest Threat Intelligence:** Stay abreast of the latest threat reports and intelligence feeds. This requires a proactive approach to gathering and analyzing information on emerging threats and understanding adversaries' tactics, techniques, and procedures (TTPs).

- b. **Analyze and Drive Understanding of Threat Landscape:** Understanding your industry's threat actors and techniques will help you decide on and develop threat scenarios for your organization. If you understand who has " Intent + Capability + Opportunity," you'll be better positioned to mitigate the risk.
- c. **Focus on Mimicking Current, Relevant Attack Techniques:** Prioritize emulating attacks that pose the most significant risk to your organization. This targeted approach ensures Red Team efforts align with the most probable and impactful threat vectors.

Scenario-Based Testing: Creating various attack scenarios tests the resilience of an organization's security controls across multiple security domains. RedTeaming != Pentesting. Scenario-based testing is targeted versus scan and try everything in random order to see what breaks.

- a. **Develop Diverse and Evolving Attack Scenarios:** Construct scenarios that range from straightforward phishing attacks to complex, multi-stage APT (Advanced Persistent Threat) simulations. These scenarios should test every aspect of the organization's defenses, challenging technical controls and human factors.
- b. **Test Different Aspects of Security Controls:** Ensure that testing encompasses a broad spectrum of security measures, including network security, application security, endpoint protection, and the effectiveness of employee security awareness training. This holistic approach identifies gaps in both technology and process.
- c. **Utilize Different Perspectives:** Consider injecting assumed breaches or different vantage points such as appliances, DMZs, and paths less commonly covered than endpoints. The last several years have highlighted edge devices being insecure and ripe for 0-day mass exploitation.

Purple Teaming Collaboration: The synergy between Red and Blue Teams (defensive security) enriches the security posture with insights from both offensive and defensive perspectives.

- a. **Foster Collaboration with the Blue Team:** Establish regular communication channels and collaborative exercises between Red and Blue Teams. This collaboration turns insights into actionable intelligence, enhancing the organization's ability to respond to and mitigate real threats. This collaboration helps foster trust between teams and will ensure that the organization's defenders listen and respond to your recommendations, not just dismissing them outright.
- b. **Share Insights, Findings, and Mitigation Strategies:** Create a feedback loop where findings from Red Team operations are systematically shared with the Blue Team and vice versa. This exchange not only informs better defense mechanisms but also refines future Red Team operations based on the most effective strategies against the organization's defenses.

Optimizing Red Team operations is a dynamic and continuous process. By focusing on these key areas—tool selection, threat emulation, scenario testing, and collaboration—organizations can ensure that their Red Team operations provide tangible, impactful contributions to their overall cybersecurity posture. This strategic approach transforms Red Team activities from isolated exercises into integral components of a comprehensive, adaptive security strategy.



PHASE 3

Elevating Program Efficacy

With a solid operational framework in place, the focus shifts to elevating your Red Team's capabilities. This stage is about adopting advanced techniques and tools to simulate sophisticated cyber threats more effectively. Elevating your Red Team involves staying abreast of the latest in cyber threat intelligence, advanced persistent threats (APTs), and emerging technologies. It also includes enhancing your team's skills in areas such as social engineering, physical penetration testing, and digital intrusion techniques to cover the full spectrum of potential threats.

This roadmap section focuses on elevating your Red Team's capabilities through strategic threat intelligence integration, mastering advanced adversarial tactics, leveraging artificial intelligence (AI) and machine learning (ML), and developing a cyber range for enhanced training and testing.

Threat Intelligence Integration: The dynamic nature of cyber threats requires Red Teams to be adaptable, constantly updating their strategies to reflect the latest adversary behaviors and exploit methodologies.

- a. **Incorporate Real-Time Threat Intelligence Feed:** Choose tools that can emulate a wide range of real-world threats, such as Breach and Attack Simulation (BAS) tools like SCYTHE, AttackIQ, Picus, or others. These tools should allow Red Teams to simulate sophisticated cyber-attack scenarios across various vectors, including email, web, and endpoint.
- b. **Adjust Tactics Based on Emerging Threats and Vulnerabilities:** Adapt and refine Red Team operations in response to new information. This may involve changing target selection, modifying attack vectors, or employing new exploitation techniques to ensure testing remains relevant and challenging.

Advanced Adversarial Tactics: To truly test an organization's defenses, Red Teams must think and operate like their most sophisticated adversaries.

- a. **Master Advanced TTPs:** Dive deep into advanced techniques such as living-off-the-land (LotL) tactics, where attackers use legitimate tools present in the victim's environment to conduct their operations, and n-day exploits, which involve attacking vulnerabilities not yet known to software vendors or defenders.
- b. **Emulate Nation-State or APT Group Behaviors:** By simulating the behaviors and tactics of specific nation-state actors or advanced persistent threat (APT) groups, Red Teams can provide a realistic assessment of how well an organization can withstand targeted attacks from competent adversaries.

AI and Machine Learning: Applying AI and ML in Red Team operations can significantly enhance the team's capability to conduct sophisticated, large-scale penetration tests.

- a. **Leverage AI-Driven Tools for Evasion and Detection Testing:** Use AI-based tools to automate the creation and execution of attacks that can evade detection by traditional security measures, providing a more stringent test of an organization's detection and response capabilities.
- b. **Analyze Large Datasets to Uncover Patterns and Vulnerabilities:** Employ ML algorithms to sift through large volumes of data generated by security systems and network traffic. This analysis can reveal hidden patterns, correlations, and vulnerabilities attackers might exploit. Some examples include:
 - **Intrusion Detection Systems (IDS):** ML algorithms can be used to analyze network traffic data to identify unusual patterns that may indicate a cyberattack. For example, the KDD Cup 1999 dataset is a widely used benchmark dataset for evaluating intrusion detection systems.
 - **Phishing Detection:** ML models can analyze large datasets of email content to identify phishing attempts. Features such as the frequency of certain words, the structure of URLs, and the use of HTML tags can be used to train models to distinguish between legitimate emails and phishing attempts.
 - **Anomaly Detection in Network Traffic:** ML algorithms can be used to analyze network traffic data to identify anomalies that may indicate a security breach. Techniques such as clustering and outlier detection can be used to identify unusual patterns of network traffic.

Cyber Range Development: A cyber range provides a simulated environment where Red Teams can hone their skills and test complex attack scenarios without risking real network environments.

- a. **Create a Dedicated Cyber Range Environment for Realistic Training and Testing:** Develop a virtual environment replicating an organization's critical IT infrastructure, applications, and services. This controlled setting allows for the safe execution of attacks, ranging from simple penetrations to sophisticated, multi-layered breaches. In most cases, this is a must have, as most organizations won't allow in production environments due to the perceived (or real) risk.
- b. **Simulate Complex Attack Scenarios in a Controlled Environment:** Use the cyber range to conduct exercises that mimic real-world attack campaigns, including those requiring stealth, persistence, and lateral movement within the network. This realistic approach to training and testing sharpens the Red Team's skills and prepares them for actual engagement scenarios.

Elevating your Red Team involves a continuous commitment to innovation, learning, and adaptation. By integrating real-time threat intelligence, mastering advanced adversarial tactics, leveraging the latest in AI and ML technologies, and developing a comprehensive cyber range, Red Teams can significantly enhance their effectiveness. This elevated approach strengthens an organization's defensive posture and ensures it remains resilient against the most advanced and persistent threats.



PHASE 4

Sustaining Your Program

The final stage is about sustaining and continuously improving your Red Team operations. In the fast-paced world of cybersecurity, stagnation means falling behind. Sustaining your Red Team's effectiveness requires ongoing training, adopting new and innovative testing methodologies, and constantly evaluating and updating your cybersecurity strategies based on the latest threat landscapes. This stage ensures that your Red Team remains a dynamic and evolving component of your organization's cybersecurity framework, capable of responding to new challenges as they arise.

Here's how organizations can ensure their Red Team operations are maintained and thrive over time.

Continuous Training and Skill Enhancement: The cybersecurity landscape is in constant flux, necessitating Red Team members to continually sharpen their skills and expand their knowledge.

- a. **Invest in Ongoing Training:** Allocate resources for regular training programs, workshops, and certifications. This investment helps Red Team members stay at the forefront of offensive security techniques and emerging cybersecurity technologies.
- b. **Stay Updated on the Latest Security Trends and Techniques:** Encourage Red Team members to participate in cybersecurity forums, conferences, and communities. Staying informed about the latest security trends and adversary tactics ensures the team's efforts are current and comprehensive. Teams will need to develop a process to ingest CTI and make a backlog of things to research and operationalize.

Metrics and Key Performance Indicators (KPIs): To demonstrate the value and impact of Red Team operations, it's essential to systematically measure and report on their performance.

- a. **Establish Measurable KPIs:** Define clear, quantifiable KPIs that reflect the objectives of Red Team activities. These include the number of exploitable or meaningful vulnerabilities identified, the time taken to breach critical assets, time from initial access to post-access detection, or the percentage of issues remediated based on Red Team findings.
- b. **Regularly Report Findings, Risks, and Progress to Stakeholders:** Develop a structured reporting framework to communicate the outcomes of Red Team operations. These reports should highlight critical findings, assess risks, and track progress over time, providing stakeholders with insights into the effectiveness of the organization's cybersecurity measures.

Threat Debrief and Actionable Recommendations: Following each assessment or operation, it's crucial to translate findings into actionable insights to strengthen the organization's security posture.

- a. **Provide Actionable Recommendations for Mitigating Identified Risks:** After every Red Team exercise, compile a detailed report outlining specific, actionable recommendations for addressing the vulnerabilities and risks identified during the assessment.
- b. **Work Collaboratively with the Blue Team to Address Vulnerabilities Promptly:** Foster a collaborative environment where Red and Blue Teams work together to understand the implications of findings and implement remediations effectively. This partnership ensures a more resilient and responsive security framework.
- c. **Incorporate Lessons Learned into Future Assessments:** Use the insights gained from each Red Team exercise to refine and enhance subsequent assessments. The organization can stay ahead of evolving threats and improve its overall security strategy by continuously updating tactics, techniques, and procedures based on real-world findings. This iterative approach to security ensures that defenses are always aligned with the latest threat landscape.

Regulatory Compliance: Ensuring Red Team operations adhere to relevant regulations and legal requirements is critical for maintaining organizational integrity and trust.

- a. **Comply with Industry Regulations and Legal Requirements:** Understand and align Red Team operations with all applicable legal, regulatory, and industry-specific requirements. This alignment is essential for avoiding legal issues and demonstrating a commitment to responsible security practices.
- b. **Document Adherence to Avoid Potential Legal Issues:** Maintain comprehensive records of all Red Team activities, including the scope of operations, methodologies employed, and adherence to established rules of engagement. This documentation is evidence of compliance and can be critical in legal scrutiny.

Engage External Assessors: Bringing in third-party assessors provides an independent perspective on the organization's security posture, offering insights that might be overlooked internally

- a. **Periodically Engage Third-party Assessors for Independent Validation:** Schedule regular assessments by external cybersecurity firms to validate the effectiveness of Red Team operations and the organization's overall security measures.
- b. **Gain Fresh Perspectives on Your Security Posture:** External assessments can reveal new vulnerabilities, validate the effectiveness of current defenses, and provide recommendations for enhancing security practices, offering fresh insights that contribute to continuous improvement. Even the best internal red teams should engage with external red teams to get a new perspective and set of TTPs, as the cadence for consulting red teams is different from internal.

Sustaining Red Team operations is a multifaceted endeavor that requires ongoing attention to training, performance measurement, regulatory compliance, and integrating external perspectives. By committing to these principles, organizations can ensure that their Red Team remains invaluable in the quest for robust cybersecurity defenses.

Conclusion & Recommendations

Red Teaming is a critical pillar within contemporary cybersecurity frameworks and a mature security program, adopting a proactive stance in identifying and neutralizing potential threats well ahead of actual exploits by adversaries. This eBook has charted a comprehensive path from establishing a robust foundation for Red Team operations to their operationalization, enhancement of capabilities, and ongoing support and refinement.

To effectively leverage Red Teaming within your cybersecurity strategy and ensure a state of preparedness against both current and emerging threats, consider the following recommendations:

1. **Continuous Skill Development:** Invest in regular training and professional development for your Red Team members to keep pace with the latest cybersecurity trends, tools, and techniques. Encourage participation in cybersecurity conferences, workshops, and simulations that challenge and expand their skill sets.
2. **Adopt a Holistic Approach:** Ensure that Red Teaming activities are integrated with your overall cybersecurity strategy, working with other security measures and teams. This includes fostering a collaborative environment with Blue Teams (defensive security) to share insights and implement improvements more effectively via Purple Teaming.
3. **Leverage Real-Time Intelligence:** Incorporate up-to-date threat intelligence into Red Team operations to simulate the most relevant and pressing threats. This approach ensures that your security measures are tested against scenarios that mirror real-world risks.
4. **Emphasize Scenario-Based Testing:** Develop and execute a diverse range of attack scenarios that cover various aspects of your organization's security posture. This should include both technical and human elements, from system vulnerabilities to social engineering tactics.
5. **Regularly Review and Update KPIs:** Establish clear, measurable KPIs to assess the impact of Red Team operations and continuously review and adjust these KPIs to align with evolving security objectives and threat landscapes.
6. **Ensure Compliance and Documentation:** Maintain rigorous documentation of Red Team activities, methodologies, and findings to demonstrate compliance with regulatory requirements and support ongoing security improvements.
7. **Engage with External Experts:** Periodically involve external cybersecurity assessors to independently evaluate your security posture. This external perspective can unveil new insights and validate the effectiveness of your Red Team's efforts.
8. **Create a Cybersecurity Culture:** Use insights and learnings from Red Team activities to foster a culture of cybersecurity awareness across the organization. Engaging all employees in security practices strengthens your defense against threats.

By adhering to the strategies and methodologies presented—from the initial setup and enhancement of tools and techniques to the integration of advanced technologies and adherence to regulatory standards—organizations can fortify their defenses against the current threat landscape. This enhances the organization's ability to detect and respond to immediate threats and prepares it to effectively confront future cybersecurity challenges.

References

SCYTHE Adversarial Emulation Platform (<https://scythe.io/platform>)

SCYTHE Purple Team Guide (<https://scythe.io/purple-team-guide>)

MITRE ATT&CK Framework (<https://attack.mitre.org/>)

Sigma Rules (<https://github.com/SigmaHQ/sigma>)

Cyber Kill Chain, MITRE ATT&CK, and Purple teaming (<https://www.sans.org/blog/cyber-kill-chain-mitre-attack-purple-team>)

Hands-on Workshops for Purple Teaming, Detection Engineering, Weaponizing Sigma, and OT/ICS (<https://scythe.io/workshops>)

Learn more at scythe.io



SCYTHE

6751 Columbia Gateway
Columbia, MD 2104
info@scythe.io

About SCYTHE

SCYTHE represents a paradigm shift in cybersecurity risk management, empowering organizations to Attack, Detect, and Respond efficiently. The SCYTHE platform enables adversarial emulation, security controls validation, and aid in the collaboration between red, blue, and purple teams to improve their security posture.

