SCYTHE

CYBER FITNESS GUIDE

STRENGHTENING YOUR CYBER POSTURE

Annual Cybersecurity Fitness eGuide

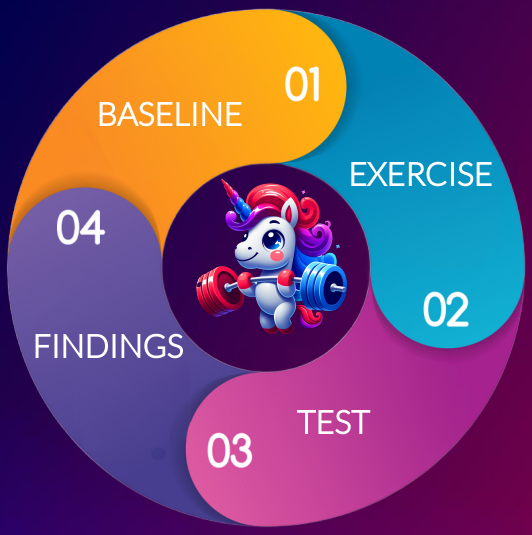
BY **SCYTHE**

Introduction

Maintaining a robust cybersecurity posture is crucial for organizations of all sizes. This annual cyber fitness guide is designed to help you baseline your cyber risk, validate cyber hygiene, assess your cyber readiness across the cyber kill chain, including ransomware readiness, analyze annual findings, and prepare for your next period.

By following this SCYTHE guide, your organization can develop a tailored cyber fitness strategy that aligns with your unique needs and goals. Annual strategy should focus on continual risk assessment, improvement, and readiness.

We hope you enjoy this eGuide.



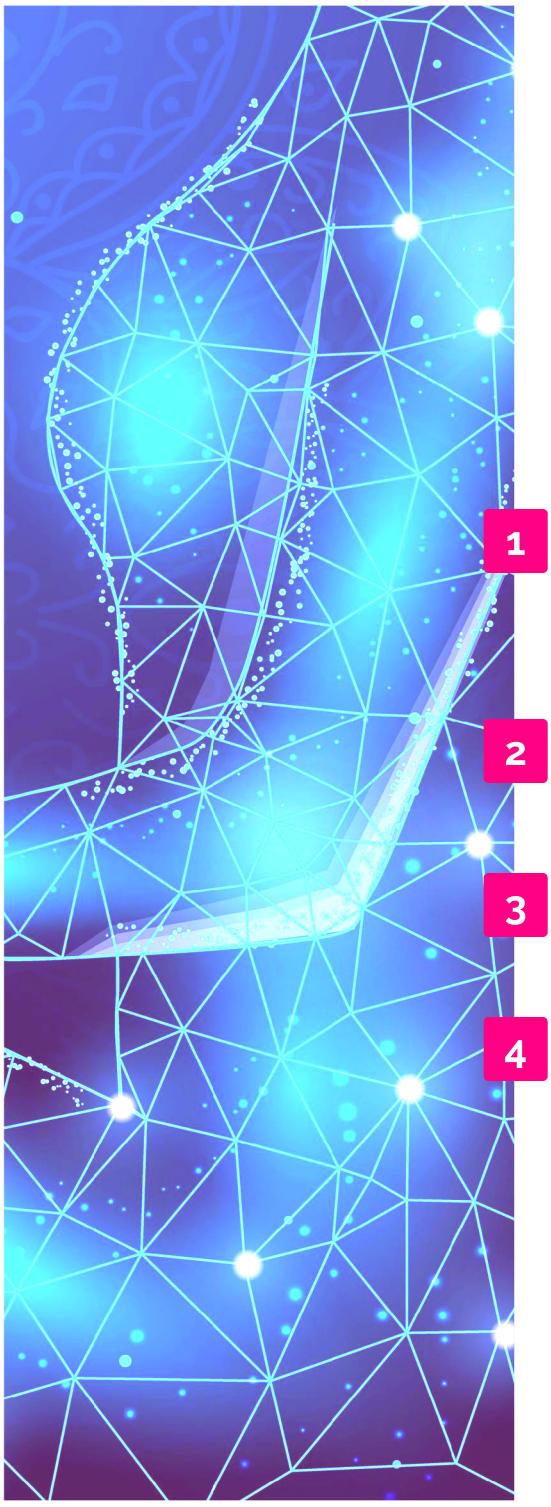
Annual Workout Plan

01 BASELINE
Risk Assessment + Hygiene

02 EXERCISE
Attack, Assess, and Mitigate

03 TEST
Ransomware Preparedness

04 FINDINGS
Analyze, Report, and Prepare



01: Baseline

Phase 1, baselining your cyber hygiene and risk should involve broad support from IT, security, compliance, and risk management teams. This phase should take **approximately 3 months**.

Key tasks to complete this include:

- Organize and categorize the various components of cybersecurity into a structured and easily understandable format (e.g., The Cyber Defense Matrix by Sounil Yu).
- Conduct a comprehensive risk assessment to identify potential vulnerabilities, exposures, and weaknesses that elevate your risk (via Purple Team Exercise).
- Utilize SCYTHE's pre-packaged content to validate cyber hygiene across your endpoints (via SCYTHE platform).
- Develop a plan to address identified risks and hygiene gaps, including third-party vendor access.

Metrics/KPIs:

- Number of identified exposures and misconfigurations.
- Percentage of controlled assets vs new/rogue.
- Tracking current vs expired agreements and licenses.
- Percentage of critical systems meeting cyber hygiene standards.

02: Exercise

Phase 2, organizational exercise. This phase should involve red security teams , purple teams, incident response and security operations. This phase should take **approximately 3 months**.

Key tasks to complete this include:

- Emulate attacks (tailored to your organizational needs) across the cyber kill chain using SCYTHE campaigns.
- Assess the effectiveness of security controls.
- Report findings and develop mitigation strategies.
- Repeat Threat Emulations to test fix-actions and assess new procedures.

Metrics/KPIs:

- Number of successful attack simulations.
- Number of TTPs undetected, logged, alerted, or blocked.
- Percentage of security controls effective at each kill chain stage.
- MTTD and MTTR

03: Test

Phase 3, testing your ransomware readiness. This phase should involve your entire security team, orchestrated via purple team exercise (PTE), and can be **accomplished within 1-2 weeks**.

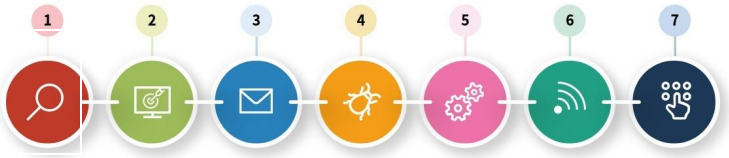
Key tasks to complete this include:

- Conduct a targeted ransomware readiness assessment using SCYTHE with a combined PTE + TTX.
- Evaluate the organization's ability to detect, respond to, and recover from ransomware attacks.
- Assess and update incident response and business continuity plans based on findings.

Metrics/KPIs:

- Time to detect and respond.
- Percentage of ransomware TTPs undetected, isolated or blocked by attack type/actor.
- Recovery time objective (RTO) and recovery point objective (RPO) for critical systems.

CYBER KILL CHAIN



04: Findings

Phase 4, performing a gap analysis and incorporating lessons learned is essential for this phase, and will involve all security team plus management. This phase should take **approximately 3 months**.

Key tasks to complete this include:

- Perform gap analysis, reviewing incidents and assessment findings.
- Discuss corporate security initiatives, industry trends and potential threats.
- Determine budget required to address gaps and new threats

Metrics/KPIs:

- Reduction in vulnerabilities and incidents
- Progress on security initiatives

Learn more at **scythe.io**

SCYTHE
6751 Columbia Gateway
Columbia, MD 21046
info@scythe.io

About SCYTHE

SCYTHE represents a paradigm shift in cybersecurity risk management. SCYTHE enables teams to elevate security resilience via insights gained through adversarial emulation and controls validation.