ADVANCED CYBER SECURITY CENTER
COLLABORATIVE DEFENSE • TRUSTED NETWORKS

BEYOND COMPLIANCE

PENETRATION TESTING, RED AND PURPLE TEAMS: CONTINUOUS ASSESSMENT TO IMPROVE SECURITY AND BUILD TALENT

DECEMBER 2020

CONTINUOUS ASSESSMENT MATURITY MODEL

RESEARCH PAPER

Please see the model's companion 2020 report, **Penetration Testing, Red and Purple Teams: Continuous Assessment to Improve Security and Build Talent.** Based on ACSC member interviews and focus groups, the report examines how organizations are using these assessment strategies, including cyber risk inputs to set priorities, benchmarks and metrics for results, costs and the talent agendas and vendor options. **Click to view.**

ABOUT THE AUTHORS

AUTHOR

John McKenna is President and CISO Chair of the ACSC and the former SVP and Global CISO of Liberty Mutual

ADDITIONAL SUPPORT

William Guenther is the Executive Chairman of the ACSC and Chairman, CEO and Founder of Mass Insight Global Partnerships

Kathryn Plazak, Plazak Associates

GRAPHIC DESIGN

Sarah Waters, Sarah Beth Graphics

ABOUT THE ACSC

The Advanced Cyber Security Center (ACSC) is the region's only non-profit, member-driven organization committed to strengthening member cybersecurity defenses and preparing the region's response to large scale cyber threats. The ACSC was established in 2012, as a 501(c)3 organization and was the model for Information Sharing and Analysis Organizations (ISAOs) when Presidential Executive Order 13691 was implemented in 2015. Currently the ACSC has 27 members representing the financial services, healthcare, technology and other sectors, along with leading universities, the Federal Reserve Bank of Boston and the Commonwealth of Massachusetts.

I. BASIC FUNDAMENTALS FIRST

Entry to the Continuous Assessment Maturity Model requires that three basic security fundamentals are in place first as a foundation:

Up-to-date essential system hygiene practices are a critical pre-condition to justifying the investment in assessments beyond what is required by regulators and third parties. That means:

a. asset management practices are in place,

b. important systems are up to date for "patches" available from vendors, and

c. vulnerability scanning and remediation is practiced, with awareness of and plans for closing gaps in consistency and completeness.

Methods established for setting risk priorities, measuring results and progress; this could include standard framework/dashboard (e.g., NIST/CSF, CIS controls, internally customized dashboard).

An established Blue Team (either internal or outsourced) and security incident response plan that is routinely tested and updated with table top walk-throughs, continually monitoring and defending company networks systems. And assure Blue Teams have incorporated the latest tools before putting them into battle.

II. FIVE STEPS TO MATURITY

FIVE STEPS TO ESTABLISH A PEN TESTING, RED AND PURPLE TEAM PROGRAM

As a baseline, ensure that you have basic hygiene practices in place, especially for your most critical assets, and that you continue to improve these practices as gaps are known and prioritized.

STEP ONE - DEFINE VISION AND STRATEGY

Define vision and strategy over the next 3-5 years, assessing talent and capacity, building a roadmap with internal vs. external responsibilities, and funding requirements.

STEP TWO - BUILD EXECUTIVE SUPPORT

Build executive support and acquire funding for moving beyond a “compliance-driven” practice, using company stories, metrics and marketplace research to demonstrate how company’s risk will be reduced, and sharing your roadmap for success.

STEP THREE - ADOPT A FRAMEWORK

Adopt a framework or dashboard and mechanisms to identify goals and priorities, measure results, and track progress of improvements.

STEP FOUR - DEFINE AND IMPLEMENT

Define and implement a change management and communication program that enlists the support of stakeholders, especially those who may feel threatened or whose engagement is essential, educating them that this is a joint mission of reducing risk and protecting the company.

STEP FIVE - PLAN ON SIMPLE STEPS AND EARLY WINS

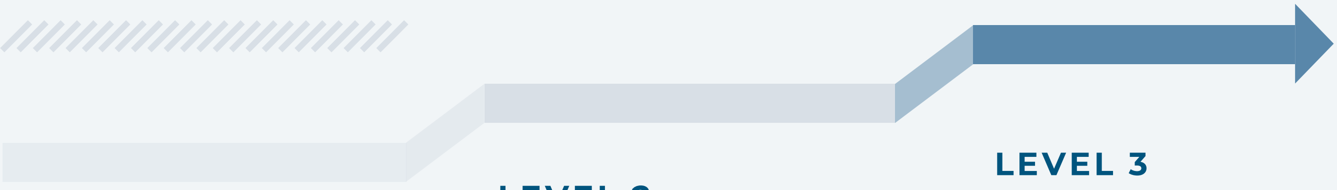
Plan on simple steps and early wins over the first 6-12 months, and communicate progress and results often with executives and stakeholders, demonstrating the impact in business terms, to sustain support and funding.

III. CONTINUOUS ASSESSMENT MATURITY MODEL SUMMARY

DEFINITIONS AND ASSUMPTIONS

Based on an examination of member company best practices, we have created a simple and flexible maturity model as a practical tool to help organizations move beyond "check the box" compliance in order to improve security and build talent.

The intent of this maturity model is to guide members through three levels, advancing their security testing programs along a progression of maturity.



LEVEL 1

Planning or early stages of definition and implementation

LEVEL 2

Practices defined and implemented, with capabilities evolving and coverage expanding

LEVEL 3

Capabilities are advanced, and coverage is broad and consistent

Maturity Model Progression for Continuous Assessment

With basic security hygiene as the entry point to go beyond "check the box" compliance and continuously improve security and build talent, these are the assessment steps to take to target improvements in an organization's systems and data security.

The model uses the following definitions.

PEN TESTING	RED TEAMS	PURPLE TEAMS
An authorized pre-defined, simulated cyberattack performed to evaluate the security of a system	Teams of attackers – termed "ethical hackers" – or automated attack platforms	Collaborations and joint meetings of the Red and Blue Teams after exercises or at other times to assess vulnerabilities and develop short- and medium-term improvements in security

CONTINUOUS ASSESSMENT MATURITY MODEL SUMMARY: PARTS A AND B

A. ASSESSING SYSTEMS AND PROCESSES

→ INTERNAL RESOURCES EXPAND →

LEVEL 1 - PEN TESTING

Directed and **limited testing of discrete standard controls** to identify vulnerabilities

Primarily **driven by compliance**

Typically a defined **scope and time-limited**

No talent building

LEVEL 2 - RED TEAMS

More active, **open-ended, and ongoing**

Attacks span **systems eco-system**

Higher level testing of vulnerabilities using **attack simulation tools**

Starts to build Blue Team staff capacity

LEVEL 3 - PURPLE TEAMS

Integrated strategy to test/respond quickly to vulnerabilities

Collaboration of Blue and Red Teams **builds talent and culture**

Expands **detection and response capacity**

Intel, risk, architects and engineers at table to shape attacks, architect solutions

**THIS MODEL IS NOT BASED ON SDLC APPLICATION TESTING.

B. ASSESSING AND BUILDING MANAGEMENT, TALENT AND CULTURE

As organizations move from Pen Testing to Red Teams and Purple Teams, they will also realize benefits in the talent and skills development of their teams.

LEVEL 1 - PEN TESTING

Staff **trained primarily by external programs** (e.g. SANS)

Advanced testing by external parties with internal participation provides some learning opportunities

LEVEL 2 - RED TEAMS

Some internal experienced tech staff

Range exercises and “Capture the Flag” events used periodically to build talent

Broad range of talent tested/improved in exercises: SOC ops/analyst, management and collaboration, physical security, employee vigilance, cyber culture

LEVEL 3 - PURPLE TEAMS

Sophisticated technical skills on staff engaged in Red/Blue/Purple Team exercises for talent development, assessment

Extends beyond security: **Range exercises used regularly** to learn new TTP’s, improve response timing and capacity

Purple Teams build solutions culture; architects, engineers, developers, risk, privacy, legal, communications, employees, physical security

IV. FULL CONTINUOUS ASSESSMENT MATURITY MODEL

DEFINITIONS AND ASSUMPTIONS

Moving Beyond “Check the Box” Compliance to Continually Improve Security and Built Talent

We examined how organizations are using penetration testing and Red Team exercises to improve their security and build talent. Based on this research we have created a simple and flexible maturity model that will guide members as they look to advance their security programs.

The intent of this maturity model is to guide members through three levels of advancing their penetration testing and Red Team programs. First, some definitions and assumptions:

HYGIENE

Basic security hygiene practices are in place. They may include vulnerability management and security assessments by external parties against industry frameworks.

MATURITY

The maturity levels presented are generally stated. Your organization’s current state plans and investment priorities will vary based on organization size, industry sector, geographic scale and company policy/philosophy on risk.

MATURITY LEVELS

The maturity levels are intended to be simple progressions:

Level 1

Planning or early stages of definition and implementation

Level 2

Practices defined and implemented, with capabilities evolving and coverage expanding

Level 3

Capabilities are advanced, and coverage is broad and consistent

IMPACT

Impact is relative in the context of these practices, indicated by the security shield icons, and will vary based the maturity levels of other dimensions of your security program.

🛡	**LOW**
🛡🛡	**MEDIUM**
🛡🛡🛡	**HIGH**

COSTS

Cost is indicated in ranges and will vary based on organization size, scale of team and implementation, investment strategies, etc. (Also consider using percentage of security budget as a metric for levels.)

$	**Less than $100,000**
$$	**$100,000 - $500,000**
$$$	**More than $500,000**

FULL CONTINUOUS ASSESSMENT MATURITY MODEL: PARTS A AND B

A. ASSESSING SYSTEMS AND PROCESSES

Definition

LEVEL 1 - PEN TESTING

Basic and targeted assessments of system controls and technical defenses

LEVEL 2 - RED TEAM

Use of ethical hacking – dynamic, broader, and continuing assessment of system vulnerabilities

May include some level of Blue Team participation

Includes testing talent – maintaining system defenses; detection and response to attacks, etc.

LEVEL 3 - PURPLE TEAM

Formal program of Red Teams and Blue Teams collaborating on a regular basis to continually assess system vulnerabilities.

Establishes priorities of near term and long term improvements in system controls, security architecture and processes.

Builds an advanced culture of collaboration across security teams.

Trains Red Teams and Blue Teams to refine skills and develop better understanding of next generation attacks.

Assessment Methods and Frequency

LEVEL 1 - PEN TESTING

Penetration testing conducted annually, primarily on most critical systems

🛡🛡 $

LEVEL 2 - RED TEAM

Red Team penetration testing targeting most critical assets and systems, run semi-annually or quarterly

🛡🛡 $$

May include Blue Team engagement and testing of detection and response

LEVEL 3 - PURPLE TEAM

Highly collaborative Purple Team comprising Red Team/Blue team exercises are conducted weekly

🛡🛡🛡 $$

Range exercises with external parties to test and score incident responsiveness

🛡🛡🛡 $$$

A. ASSESSING SYSTEMS AND PROCESSES *CONTINUED*

Resourcing

LEVEL 1 - PEN TESTING

EXTERNAL

Testing primarily **conducted by vendors**

Limited budgets and expertise

LEVEL 2 - RED TEAM

EXTERNAL / INTERNAL

Testing initially conducted primarily by vendors, moving to **some level of internal capacity** to coordinate exercise and participate at some level in attacks

Internal talent grown to partner with vendors and establishing internal Red Team capacity

LEVEL 3 - PURPLE TEAM

INTERNAL / EXTERNAL

Full funding commitment to internal talent and capacity

Selective use of vendors based on Corporate policy on external assessments and expertise (fresh eyes)

Full engagement of architects and engineers in designing and participating in exercises

Methods for Identifying Targeted Systems

LEVEL 1 - PEN TESTING

Systems prioritized **by regulators or customers 3rd party security programs**

🛡 **$**

LEVEL 2 - RED TEAM

Issues identified by Red Team based on analysis of **highest risk assets and knowledge of adversaries**; may include use of frameworks such as MITRE ATT&CK

🛡🛡 **$$**

LEVEL 3 - PURPLE TEAM

Issues and Purple Team targets identified through a **highly collaborative engagement with risk, threat intel,** identifying highest risk assets and adversary methods using frameworks such as MITRE ATT&CK

🛡🛡🛡 **$$**

Use of Threat Intel

LEVEL 1 - PEN TESTING

Pen Test vendors draw on industry threat intel to inform annual testing

No internal threat intel program

🛡 **$$**

LEVEL 2 - RED TEAM

Red Team intel is based on external sources to target their attacks

Internal threat intel function is developing and influences targets and methods of attacks

🛡🛡 **$$**

LEVEL 3 - PURPLE TEAM

Full internal threat intel function and automated services to shape TTPs of attacks

🛡🛡🛡 **$$$**

A. ASSESSING SYSTEMS AND PROCESSES *CONTINUED*

Remediations and Actions or Findings

LEVEL 1 - PEN TESTING

Remediation of findings and failures is not consistent or complete

LEVEL 2 - RED TEAM

Remediations completed within 90 days

Longer term security engineering and architecture improvements are identified

LEVEL 3 - PURPLE TEAM

Remediations completed real time or within 30 days

Longer term security engineering and architecture improvements are launched

B. ASSESSING AND BUILDING MANAGEMENT, TALENT AND CULTURE

LEVEL 1 - PEN TESTING

Internal security analysts and management **trained primarily by external programs** (e.g., SANS)

Advanced testing conducted by **external parties with internal participation** may provide some learning opportunity

🛡 **$**

LEVEL 2 - RED TEAM

External range exercises and “Capture the Flag” events used periodically to build SOC analyst technical talent, management and collaboration skills

🛡 **$$**

LEVEL 3 - PURPLE TEAM

Sophisticated technical skills on staff engaged in **Red Team/ Blue Team exercises** for talent assessment and development

🛡🛡 **$$**

Range exercises used regularly to learn **new TTPs** and improve response timing and capability

🛡🛡 **$$**