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

RESEARCH REPORT:

THE CONTINUOUS ASSESSMENT MATURITY MODEL

Please see this report's companion framework for continuous assessment to advance your organization's Penetration Testing, Red and Purple Team programs along a maturity continuum. **Click to view.**

THE ACSC IS LOCATED AT THE MITRE CORPORATION, 202 BURLINGTON RD, BEDFORD, MA. LEARN MORE AT ACSCENTER.ORG. CONTACT INFO@ACSC.ORG

ABOUT THE AUTHORS

AUTHOR

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

ADDITIONAL SUPPORT

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

Kathryn Plazak, Plazak Associates

GRAPHIC DESIGN

Sarah Waters, Sarah Beth Graphics

RESEARCH PARTNER

With appreciation to Randori and **Brian Hazzard,** CEO, for their participation, thought leadership and support in the development of this field research.

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.

ACSC COLLABORATIVE DEFENSE RESEARCH REPORTS

This report is the fourth in a series of research reports on Collaborative Defense Practice.

2019

Cyber Incident Planning and Response: The Roles of Legal Counsels and Communications Executives at Sophisticated Organizations

Created by:
ACSC

2018

Leveraging Board Governance for Cybersecurity: The CISO/CIO Perspective

A Collaboration of:
ACSC and Mass Insight

2017

Collaborative Cyber Defense: Barriers and Best Practices for Strengthening Cyber Defense by Collaborating Within and Across Organizations

Prepared for the ACSC by:
McKinsey & Company and Mass Insight

I. RESEARCH OVERVIEW, OBJECTIVE AND METHODOLOGY

Penetration Testing (Pen Testing) and the use of Red and Purple Teams are key strategies used to assess security and further ongoing improvements. Large, sophisticated organizations as well as smaller organizations need to use continuous testing strategies.

These tests are critical to establishing and exercising business continuity operations across all functions, especially on the Information Technology side – building the "muscle memory" needed to respond effectively to serious threats.

While the most basic of these efforts satisfy regulatory requirements, what does it look like to go beyond "checking the box" compliance and develop a robust practice of penetration testing and red teaming that aligns with your individual organization?

The objective of this effective practice field research was to examine three components important to strong cyber hygiene: Penetration Testing (Pen Testing), Red and Purple Teams. The findings are based on three focus groups with ACSC member organizations, more than a dozen in-depth interviews of member CISOs and three vendors (see Acknowledgements for list), and a small sample survey.

KEY RESEARCH QUESTIONS:

Prioritization: How do member organizations prioritize business and data risks for assessments?

Continuous Assessment Programs: Do member organizations continuously test, and if so what strategies are used for continuous testing (Pen Testing, Red and Purple Teams)?

Benchmarks: What industry and/or internal benchmarks are used?

Accessing Talent and Resources: How do you best leverage your internal staff with external vendor resources, optimize your funding, and achieve desired outcomes?

CONTINUOUS ASSESSMENT MATURITY MODEL: CONTEXT

The findings of this report are presented within the context of the ACSC's Continuous Assessment Maturity Model, where we examined how organizations are using penetration testing, red and purple teams to improve their security and build talent. The maturity levels presented are generally stated as follows.

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

II. PRIORITIZATION OF RISKS AND METRICS FOR ASSESSMENTS

PRIORITIZATION OF RISKS

Prioritization is critical in deploying assessments.

Sophisticated security executives warn against too much of the wrong testing. “I’m a contrarian. We do too much undifferentiated testing. You have to be very good at defining scope, otherwise you’re paying a vendor to come and play in your networks.” And finally, “don’t test what you already know is broken.” (Unless you are using the results to make a case internally to prioritize remediation.)

Sophisticated organizations use multiple sources to determine targets for Pen Testing and shape Red and Purple Team operations:

- Data classification, identifying “crown jewels” and critical systems inventory
- Threat intel on adversaries (including internal threat evaluations based on recent history of attacks)
- Known vulnerabilities
- Commissioned or mandated assessments
- Business risk models and repositories

Regardless of the source, partnering with business units and key stakeholders in the organization to get their agreement on priorities is essential.

> **“You have to be very good at defining scope. Otherwise, it’s paying an outside firm to come into your system and play. Make it focused on your crown jewels – data or critical systems.”**

Threat Intel – from internal or external sources – is a particularly critical resource to shape vulnerability assessments and should be used by every organization to shape their programs.

Advanced organizations establish Purple Team priorities through a collaborative staff engagement with risk and threat intel, and incorporate attacker methods using frameworks such as MITRE ATT&CK.

To establish priorities and review threats, mature organizations also have regular meetings involving multiple staff functions - weekly or daily “stand up” meetings in some cases – to review threats and vulnerabilities across lines of business, which then shape vulnerability assessments. Cross-functional meetings can be large scale to distribute information widely, involving up to 75 participants in one firm. Heat maps for internal and external/ISAC feeds frame the briefings with risk scores of 1-5 attached to threats.

METRICS FOR ASSESSMENTS

Currently, limited industry benchmarks exist for continuous testing beyond annual Pen Tests required for regulatory compliance. NIST, CIS Control Framework, MITRE ATT&CK and others don't provide standards. In lieu of standards, ACSC member companies report the development of their own internal objectives. These should focus on fundamental improvements in the security systems, management and talent.

The DoD's Cybersecurity Maturity Model Certification (CMMC) is quickly evolving as a new minimum set of standards to be considered beyond just defense contractors.

Time to remediate with oversight from a Mitigation Management Team is a typical metric used by most firms. Dashboards and multi-year improvement goals tied to assessments play an important role. As one member said, "Any vulnerability finding that shows up twice now requires an explanation to the new CEO."

An organization early in continuous testing development typically does not have consistent remediation performance.

Somewhat advanced organizations will target remediations of critical vulnerabilities completed within 90 days, while very advanced organizations succeed in consistently remediating critical vulnerabilities within 30 days.

The chart below outlines some of the metrics and measures that determine where you are on the maturity continuum.

> **"'I didn't get breached' is not a metric. Metrics can be developed by tracking continuous improvement."**

Metrics and Methods Cited by Members
Within the Framework of the Continuous Assessment Maturity Model

LEVEL 1 - PEN TESTING	LEVEL 2 - RED TEAM	LEVEL 3 - PURPLE TEAM
Minimally, meet all compliance requirements	Frequency - Red Team exercises conducted each quarter	Frequency - Purple Team exercises conducted each week/month
Count/% of critical systems tested Number of critical vulnerabilities identified	Number of critical vulnerabilities identified and remediated	Number of critical risks identified and remediated
Number/% of critical findings remediated within established timeframe	Attacks detected vs. undetected by Blue Team	Attacks detected vs. undetected by Blue Team
	Calculated improvement in security posture (assumes established KPIs or scoring method)	Calculated improvement in business risk posture (assumes alignment and scoring method)

Organizations use selected metrics consistently to gain senior management buy-in for programs, and this buy-in becomes increasingly important as you move up the maturity scale.

III. CONTINUOUS ASSESSMENT PROGRAMS: DEFINITION, USE, COSTS

PEN TESTING

Definition of Pen Testing

We define Penetration Testing as:

- An authorized pre-defined, simulated cyberattack performed to evaluate the security of a system
- Involves human-led and sometimes automated 'attacks' on specific, targeted elements of data systems
- Limited duration (generally up to a week)

Routine Pen Testing as part of application development and delivery is not included in this research.

Use of Pen Testing

Pen Tests are required by compliance and regulatory bodies for almost every organization at least annually and also used more extensively by organizations with significant security concerns and more resources to assess vulnerabilities. An integral part of basic security hygiene, this step is now considered standard procedure (within the last 5 years) and largely identifies top vulnerabilities, including the top 10 OWASP security risks.

With basic security hygiene already in place, well-defined, short-term Pen Testing beyond what is required by compliance (generally through a vendor) is the first level of assessment defined by the Continuous Assessment Maturity Model.

Assessments may be ordered internally by security, risk or audit functions. Externally in addition to regulatory and compliance requirements (U.S. and international), independent audits may be required by customer/3rd party assessments.

Cyber insurance requirements and standards are also driving the use of assessments to comply with minimum standards or exceed them in order to reduce premiums.

Pen Testing Costs

Pen Testing costs vary from $15,000 to over $100,000 depending on the scale of the test. In large global organizations, Pen Testing budgets can run to $1-2 million annually with over 200 tests conducted which includes systems change and new application testing.

BUG BOUNTY PROGRAMS

A number of ACSC members report the use of Bug Bounty Programs, which can be a low cost/high value option.

RED TEAMS

Definition of Red Teams

Red Teams are teams of attackers – termed "ethical hackers" – or automated attack platforms which target data systems and an entire organization to test security systems, culture and, in sophisticated organizations, the expertise of the "blue team" defenders. They are more open-ended in scope and duration than Pen Tests and attempt to replicate the TTPs (tactics, techniques, procedures) of known attackers.

Use of Red Teams

Red Team testing is the 'next step' beyond Pen Testing and the second level of Assessment Maturity. As part of a more broad-based, open-ended, ongoing assessment to identify risks, vulnerabilities and security gaps, Red Teams focus on an organization's critical assets and systems as well as security procedures. **Sophisticated organizations give Red Teams free reign** to attack their systems without notice. One member reported initially using their Red Team to 'attack and crack' passwords and build the case for ongoing Red Team exercises. Red Teams also play an important role developing blue team talent.

The use of Red Teams is increasing as technology change continues to accelerate, and organizations search for ways to identify, measure and mitigate risk.

In a hybrid environment, vulnerability assessments using Pen Tests and Red Teams cover both the on-premises and cloud systems. The cloud vendor is generally not engaged in the assessment.

Most members say they use Red Teams for technical and non-technical testing, including social engineering techniques such as phishing exercises. While the improvement of talent is not yet a common goal, Red Teams in their mature use assess and develop better technology, systems and blue team talent. **After-action reviews are critical in collaboratively learning from the exercises and developing the human element.**

Red team exercises at more mature organizations range from quarterly to 3-4x/month depending on access to an internal team. Most, however, conduct these exercises on an annual basis.

> **"Most valuable is not what is broken but how the team responds. Does the plan work?"**

BENEFITS OF RED TEAMS

- + **Assess technology and tools across systems**
- + **Build and assess Blue Team talent**
- + **Hit places you don't expect; find your blind spots**
- + **After-action reviews shape improvement strategies**

Red Team Costs and Compensation

Costs can vary from $50,000 to over $100,000 for a vendor-run automated or team-driven test, focused broadly or on particular system functions. One vendor quoted: $75,000 for 2 testers, 3 weeks including social engineering attacks from outside the organization. More complex and ongoing tests (e.g. a year-long continuous test) can cost up to $500,000.

Competitive salaries for Red Team staff are in the $180K - $200K range. Nationally recognized staff at firms like Google Zero are making $500,000 annually. Members report government Red Team staff with appropriate skills are more likely to be mission-driven and somewhat more affordable recruits.

Internal Red Teams usually max out at 4-5 staff supported by a budget of up to $1 million. Funding for more limited red team attacks usually starts with the Risk function and shifts to security as operations and budgets increase.

As organizations move along the maturity continuum, they need to consider "build vs. buy" decisions, the related costs of each and the value of using both internal and external resources. Organizations using internal and external/vendor teams collaboratively are able to access a broader range of talent and techniques.

PURPLE TEAMS

Definition of Purple Teams

Purple Teams are joint meetings and collaborations of the Red and Blue Teams after exercises or at other times to assess vulnerabilities and develop short- and medium-term improvements in security. In a mature model after confidence-building between the Red and Blue Teams, Threat Intel staff, software developers and system architects are included to shape agendas and priorities and provide feedback to the Red and Blue Teams. True Purple Teams are not staffed separately except to support the logistics for collaborations.

Use of Purple Teams

In a mature example, a large financial services firm organizes weekly "Purple Team days", a quarterly Purple Team conference and one large exercise quarterly. Even for most large organizations, however, Purple Teams are generally in development or an aspiration.

Purple Teams also provide staff training opportunities for Red and Blue Team participants and change culture through collaboration across teams and functions. Purple Teams open the "black box" of security testing by incorporating other functions into the exercises and after action reviews.

WHY IT'S IMPORTANT – ONE MEMBER'S EXPERIENCE

One member's Purple Team Program focused initially on making quick fixes to build support for the program (i.e. easily guessed or exposed passwords). After their initial success, they made the business case for the sustained program, demonstrated its value, and earned executive support - and then brought systems developers to the table to address deeper architectural flaws. As a result, the Purple Team Program:

- Drives fundamental cultural change – employees enjoy the challenge of the exercises and the change of pace. They see their work effecting change within the organization.

- Uses MITRE ATT&CK to understand the adversary and their tools, techniques and procedures.

- Demonstrates improvement with timely solutions by being dynamic and continuous, rather than relying on an annual assessment.

- Relies on executive sponsorship – the buy-in from leadership to build a trusted team, drive change, and find the necessary resources to support it.

IV. ACCESSING TALENT AND RESOURCES

INTERNAL STAFF AND VENDORS

Internal vs. External: Resourcing Red Teams

Resource scenarios vary widely across ACSC member organizations. Some teams are made up of internal players while others rely on external support; some use a combination of both. The more active the teams are, the increased likelihood the teams consist largely of internal staff members. One smaller security organization uses regular IT staff to routinely run internal "red teaming" assessments.

However, even larger security organizations with internal teams often look to outside partners for added support, skill and fresh perspective. One financial services CISO reports leaning on external resources for "building methodology for our team and creating playbooks."

External red team resources run the gamut from automated red team platforms like Randori to the Black Hills attacker teams for hire.

> "Value of external partners to access talent, impartial perspective and a company that can understand you and your business, brings out of the box thinking."

Internal Talent:

Even smaller security organizations need **internal talent with a deep understanding of continuous assessment** to select and work with vendors. Members report ideal staff as combining both hard and soft skills including curiosity, persistence and ability to communicate tactfully. Given the rapid changes in the field, there is an expanding focus on continuing education and training.

For all organizations, talent is in short supply; creating the right corporate environment with high impact exercises and challenging opportunities to grow and develop provides a critical recruiting advantage. Member feedback shows limited opportunities for blue and red team staff to exercise off-line with peers which is viewed as an opportunity.

External Talent - Vendors

Even in large, mature security organizations, vendors play an important role working with internal staff, supplementing and building an organization's capacity, including:

- Network and system vulnerability scanning tools
- Sophisticated Pen Testing/Red Team service vendors
- Internal Red Team tools and automated "Red Team" products
- Blue Team/SOC service vendors (MSSPs)
- Blue Team/SOC Detect and Respond products (e.g., SIEM, security analytics tools, incident management tools)

V. RESEARCH PARTNERS AND USEFUL RESOURCES

RESEARCH PARTNERS

Thank you to our Research Partners

Thank you to all the ACSC member organizations for their engagement and support, which made this research and report possible. In particular, our gratitude goes to the following individuals, whose input via interviews, focus groups or other advice provided the material for this report:

Bill Brown, Abacus

CJ Cox, Black Hills

Chris Harrington, Dell

Sonia Arista, Everbridge

Mark Teehan, Harvard Pilgrim

Richard Thimble, Harvard Pilgrim

Christian Hamer, Harvard University

Chris Blow, Liberty Mutual

Anna McJohn, Liberty Mutual

Brian Riley, Liberty Mutual

Martin Bialczak, Manulife/Hancock

Tom Laroche, Manulife/Hancock

Pat McGuinness, Manulife/Hancock

Greg Thompson, Manulife/Hancock

Anthony Hannon, MassMutual

Lauren Jones, MassMutual

Kris Proto, MassMutual

Neil Clauson, Mimecast

Greg Brinkman, Munich Re

Stephanie Copp, Munich Re

Adriel Desautels, Netragard

Adam Russell, Oracle

Aaron Fosdick, Randori

Brian Hazzard, Randori

Ian Lee, Randori

Eric McIntyre, Randori

David ‘Moose’ Wolpoff, Randori

Alex Gerber, Stanley Black & Decker

Gregg Doherty, State Street

Jeremy Fountain, UMass Memorial

Greg Bosworth, VHB

Skip Thomas, VHB

USEFUL RESOURCES

Blue Team Field Manual

by Alan J. White and Ben Clark
Several members found this to be a useful guide to getting started.

MITRE ATT&CK®

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community. ATT&CK is open and available to any person or organization for use at no charge.

Blue Team Handbook: Incident Response Edition

A condensed field guide for the Cyber Security Incident

Re. 2nd Edition

by Don Murdoch GSE

PICERL

The SANS Incident Response Process PICERL is an acronym that stands for: preparation, identification, containment, eradication, recovery and lessons learned. An incident response process developed by cooperative research and education organization SANS, the PICERL methodology outlines a simple process that organizations can use to form the basis of their incident response regime.