COMMONWEALTH SECURITY OPERATION CENTER AND CYBER RANGE INITIATIVE

A nation-leading initiative propelled by the MassCyberCenter

MassCyberCenter Overview

The MassCyberCenter convenes the Massachusetts cybersecurity ecosystem to improve cybersecurity resiliency, workforce development, and public awareness within the state by developing cutting edge programs, organizing engaging events, and leading collaborative working groups

Cybersecurity Innovation and Ecosystem Development

- Cybersecurity SOC/Range Initiative
- Cybersecurity Mentorship Program
- Alternative Cyber Career Education Grant Program
- Cybersecurity Training and Education Working Group
- Jobs Board

Resiliency for the Commonwealth

(Public and Private Sector)

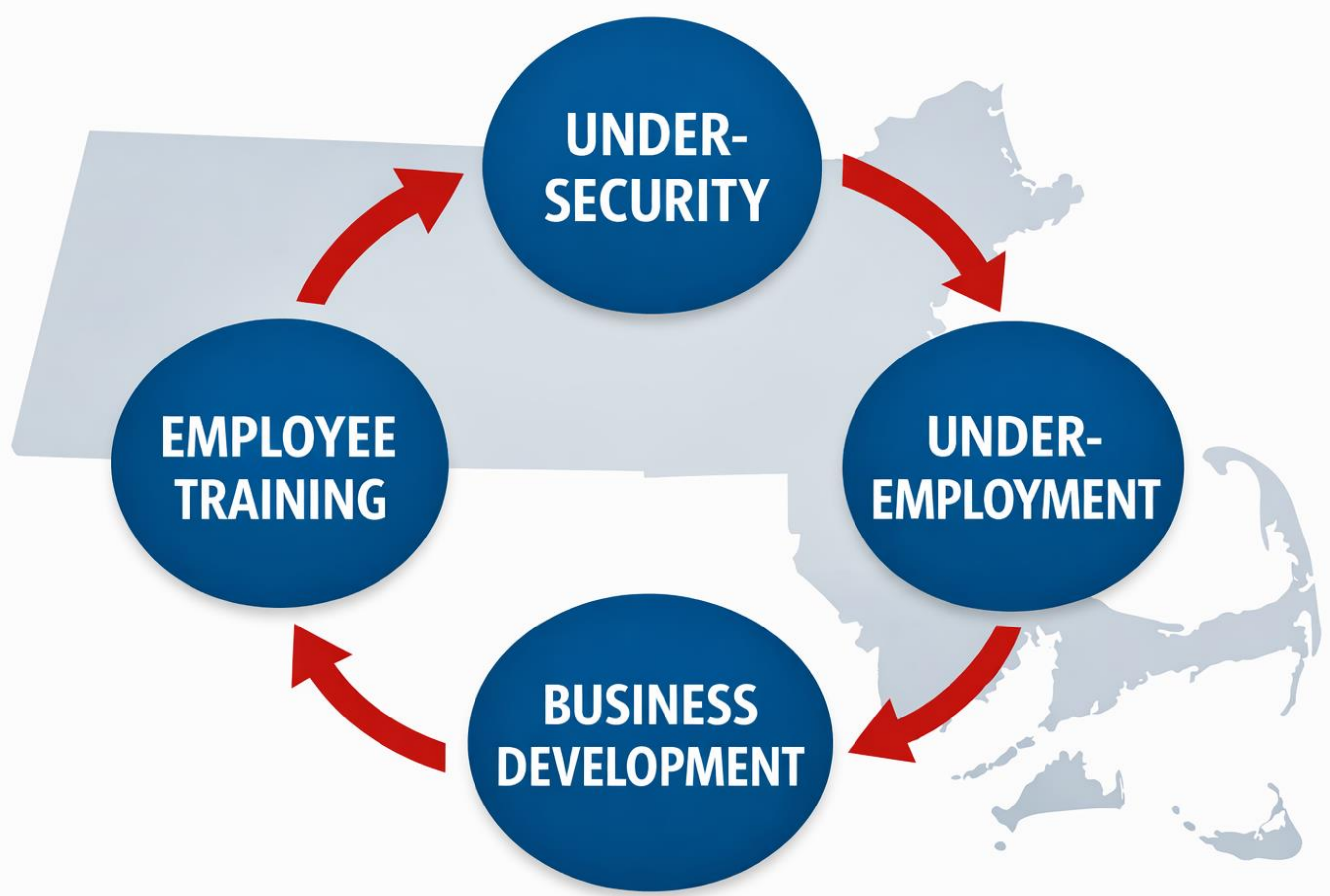
- Cyber Resilient Massachusetts Working Group
- Tabletop Exercises
- Cyber Incident Response Plan Workshops
- Resources for Municipalities
- Cyber Resilient Massachusetts Grant Program

Communication, Collaboration, and Outreach

- Massachusetts Cybersecurity Month (October)
- Citizen awareness
- Ecosystem promotion
- Talent recruitment
- National cyber events
- Webinars

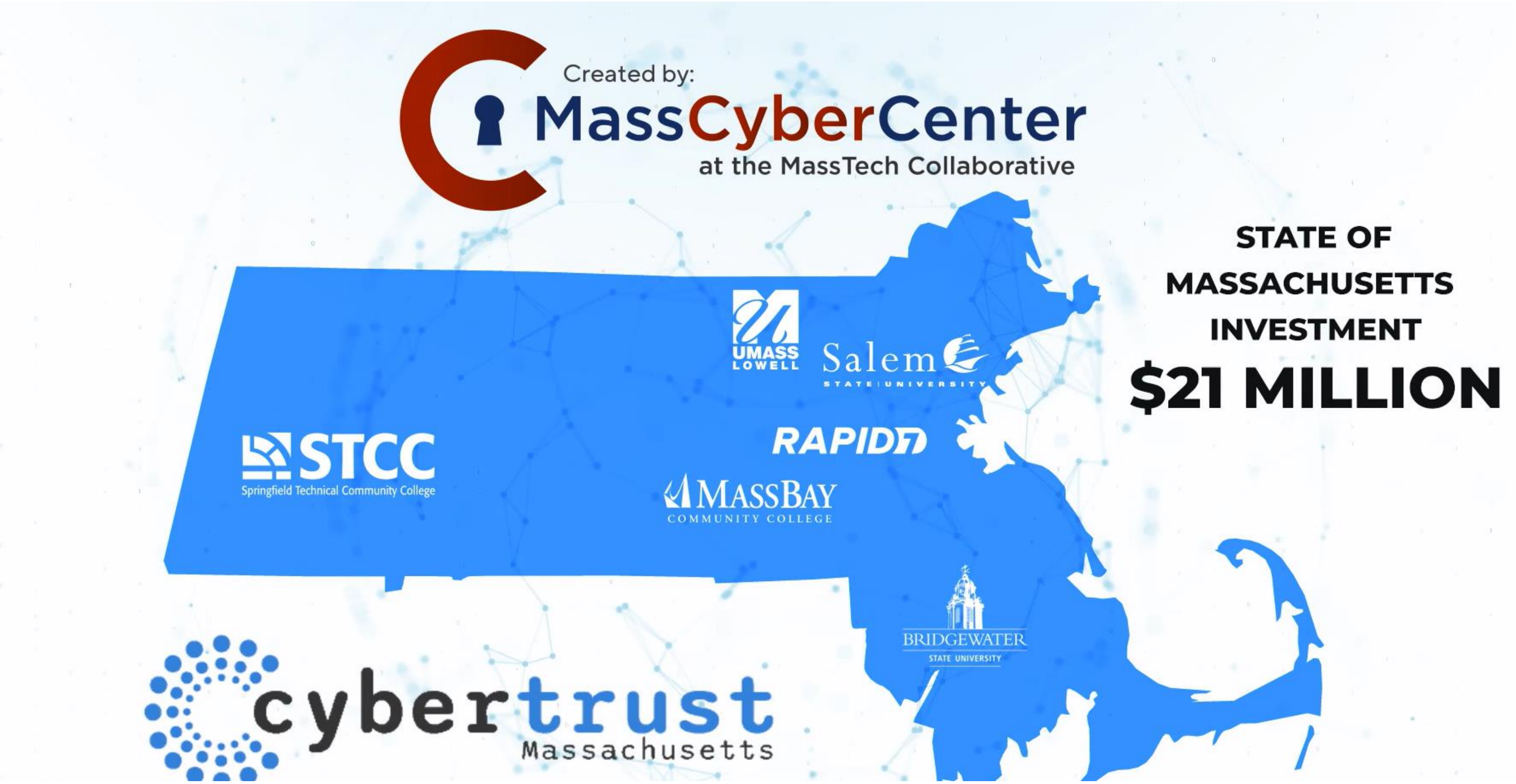
Massachusetts Cybersecurity Ecosystem Key Imperatives

The MassCyberCenter identified with its public, private, and academic stakeholders that the Massachusetts cybersecurity ecosystem needs solutions to address four key imperatives

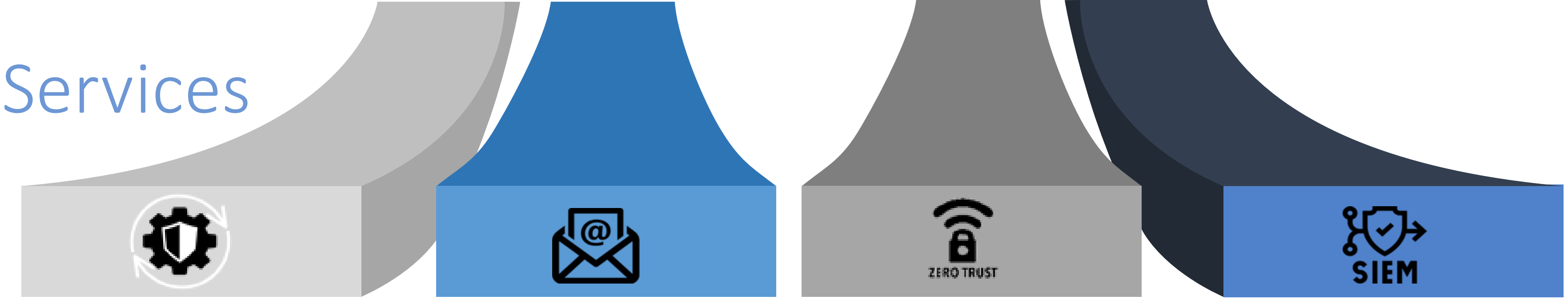


Commonwealth SOC / Range Initiative

MassCyberCenter created CyberTrust Massachusetts as the tool for delivering Security Operations Center services to municipalities, small businesses, and non-profits with the support of student employees, as well as Cyber Range services to train students to enter the workforce and upskill professionals


Created by:
MassCyberCenter
at the MassTech Collaborative
STATE OF MASSACHUSETTS INVESTMENT
$21 MILLION
UMASS LOWELL
Salem STATE UNIVERSITY
RAPID7
STCC Springfield Technical Community College
MASSBAY COMMUNITY COLLEGE
BRIDGEWATER STATE UNIVERSITY
cybertrust Massachusetts

Managed Services



MDR SERVICES

Our services give you 24/7 expert monitoring, threat detection, and fast alert resolution. We defend by correlating data across endpoints and networks to provide deeper visibility and analysis.

What You Get:

- ✓ 24/7 threat monitoring and response across endpoints, network, and cloud.
- ✓ Expert investigation and containment to stop attacks quickly and reduce impact.
- ✓ Unified visibility and reporting to strengthen your security posture and reduce internal workload.

ADVANCED EMAIL PROTECTION

Email is the primary vector for ransomware, phishing, and data theft. Our advanced filtering remediates these threats before impact.

What You Get:

- ✓ Advanced detection of phishing and email-based attacks
- ✓ Automatic removal of dangerous attachments and malicious links
- ✓ Real-time analysis of suspicious messages

APPLICATION CONTROL & ZERO TRUST SERVICES

Compromised accounts and malicious software are the most common entry points for breaches. Our advanced endpoint protection, threat intelligence, and continuous monitoring defend against exploits.

What You Get:

- ✓ Control over which applications can run on your systems
- ✓ Containment of unauthorized software and programs
- ✓ Reduced attack surface and lateral movement opportunities

LOG & ALERT CONSOLIDATION

Security events happen constantly. This service ensures you're aware of threats and have the evidence needed to investigate and prevent them.

What You Get:

- ✓ Near Real-time visibility into what's happening on your network
- ✓ Alerting of unusual behavior and potential breaches
- ✓ Activity records for compliance audits and investigations
- ✓ Faster response to security incidents

© CyberTrust 2025

CyberTrust MA – Monitoring and Response Services (Comprehensive Protection Suite)

MassCyberCenter at MassTech

More capability than most municipalities/small businesses deploy today, at a price point of less comprehensive deployments.

PRICE:

Municipal: $60

Business: $84

Managed Endpoint Detection and Response	• 24/7 monitoring of alert activity with autonomous and human response for containment and eradication • Mitigates threats, escalates only when needed • 30-minute mean time to respond (MTTR) • Best-in-class; 11 detection engines to protect from sophisticated adversary activity • Firewall control and USB device control ✓ *SentinelOne Complete Protection Platform* ✓ *SentinelOne Vigilance Respond*
Network Discovery	• Passive / active scanning; device fingerprinting • Provides network visibility; identifies rogue and unmanaged assets; creates full asset inventory of all devices on the network ✓ *SentinelOne Ranger Discovery*
Vulnerability Management	• Software inventory • Continuous and real-time visibility into application and OS vulnerabilities ✓ *SentinelOne Ranger Insights*
CyberTrust Service Plan One-time Onboarding ($2,000 fee)	• Quarterly and ad-hoc reporting on security posture and threat trend analysis including exploitable vulnerabilities and most susceptible assets • Managed agent upgrades • Prevention policy tuning and optimization • Tailored threat-hunting and custom alerts to identify early indicators of compromise

CyberTrust MA – Monitoring and Response Services (Identity Protection Option)

Sophisticated capabilities help prevent attackers from using compromised identities to leverage a compromised computer into a compromised enterprise.

PRICE:

Municipal: +$26

Business: +$36

Active Directory Hygiene	• Assesses Azure Active Directory (Entra) and On-Prem Active Directory (On-Prem AD); periodic and on-demand • Identify exposures and weaknesses in AD that attackers can target, such as misconfigured objects, Group Policies, Schema, etc. ✓ *SentinelOne Singularity Ranger AD*
Identity Detection and Response	• Deception technology for Active Directory • Make lateral movement very difficult for attackers • Protect local application credential stores to prevent misuse • Support Zero Trust ✓ *SentinelOne Singularity Identity Detection & Response*

Cyber Resilient Massachusetts Grant Program

Program Overview

Municipalities, small businesses, and non-profit organizations* are eligible to receive grants of up to $25,000 to fund Managed Detection and Response (MDR) services from CyberTrust Massachusetts for up to 3 years.

> **MassCyberCenter will prioritize applications from Massachusetts-based small businesses and non-profits that represent the ***health care and digital health sectors**

Additional Information

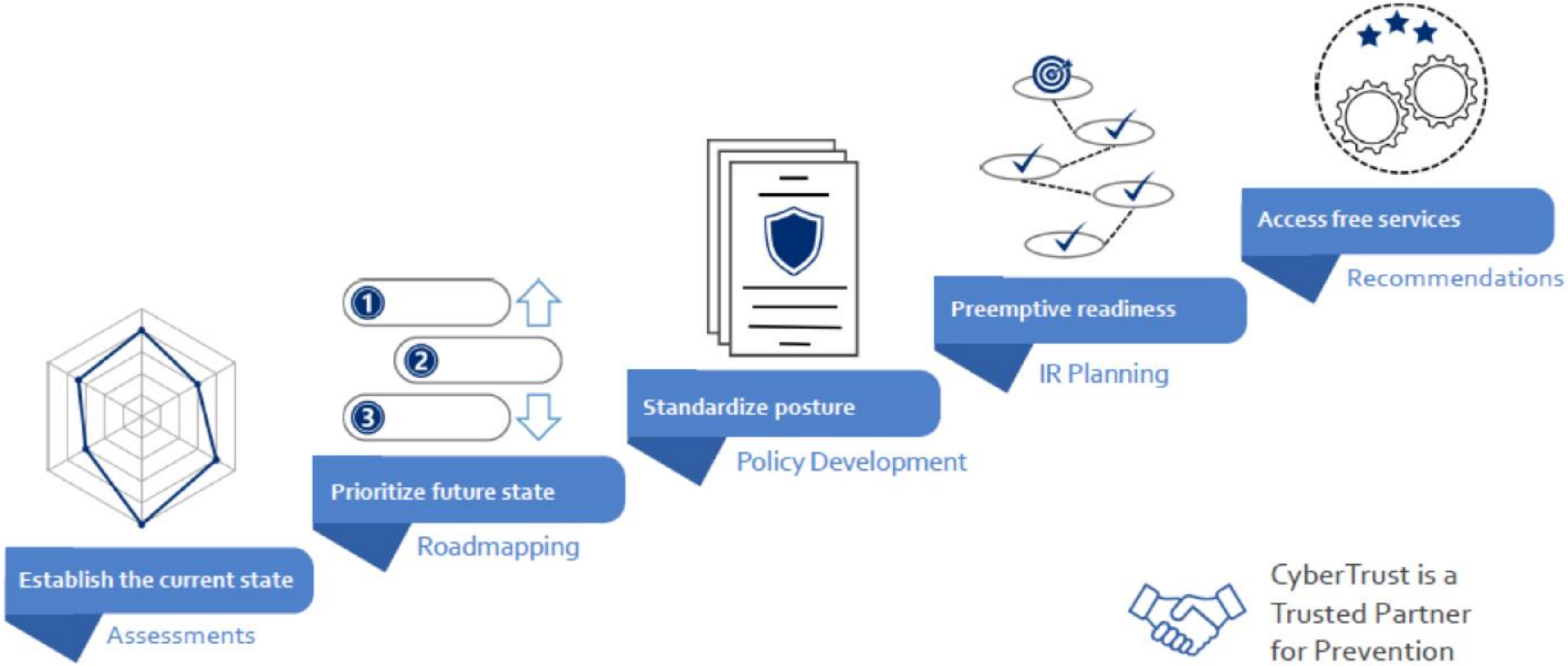
- Applications accepted on a rolling basis
- Applications must include a scope of work for MDR services from CyberTrust MA
  - Small business and non-profit respondents should contact smb@cybertrustmass.org

CyberTrust MA – Advisory Services

MassCyberCenter at MassTech

One-time service includes:

- Assessing infrastructure, security controls, practices
- Technical testing of key aspects of defenses
- Minimum set of policies and plans (including incident response plan)
- Connecting to free state or federal resources



Establish the current state

Assessments

Prioritize future state

Roadmapping

Standardize posture

Policy Development

Preemptive readiness

IR Planning

Access free services

Recommendations

CyberTrust is a Trusted Partner for Prevention

Cyber Range Program

MassCyberCenter at MassTech

Labs

Over 2300 labs broken up into topics, career paths, threat actors, CVEs, etc.

Crisis Simulation

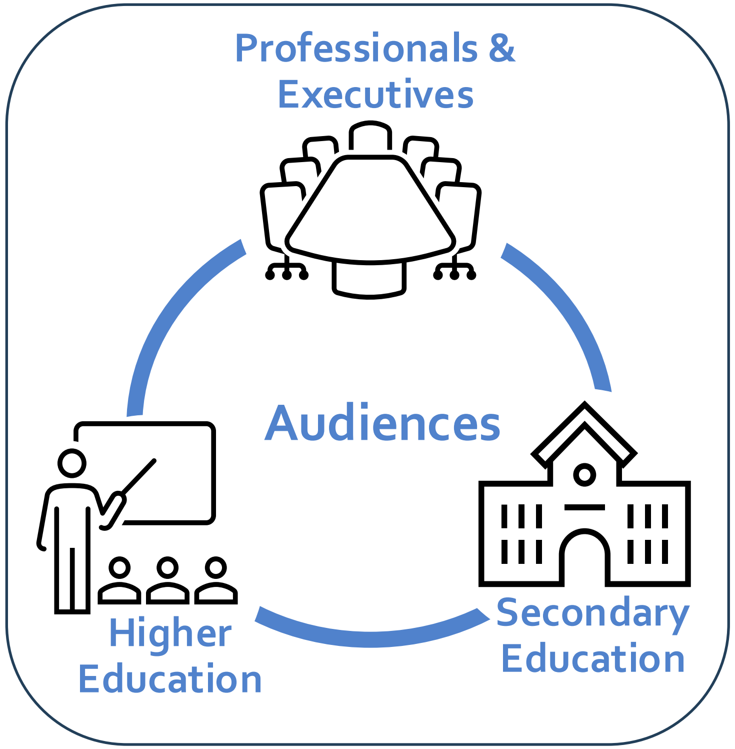
Over 60 gamified table-top scenarios for executive audiences

Team Cyber Simulation

20 end-to-end attack scenarios (offensive and defensive) to exercise team synergy and technical acumen

Candidate Screening

Baseline a potential candidate's proficiency or promotion readiness, or use as a way to assign specific content to a one-time audience (e.g. high school students)



managed by

cybertrust Massachusetts

in partnership with

IMMERSIVELABS

SOC / Range Program Outcomes (2023-Present)

63

Organizations receiving SOC services (MDR and/or Assessments)

38

Assessments (completed/pending)

30

Organizations receiving MDR services

55

SOC student interns

68

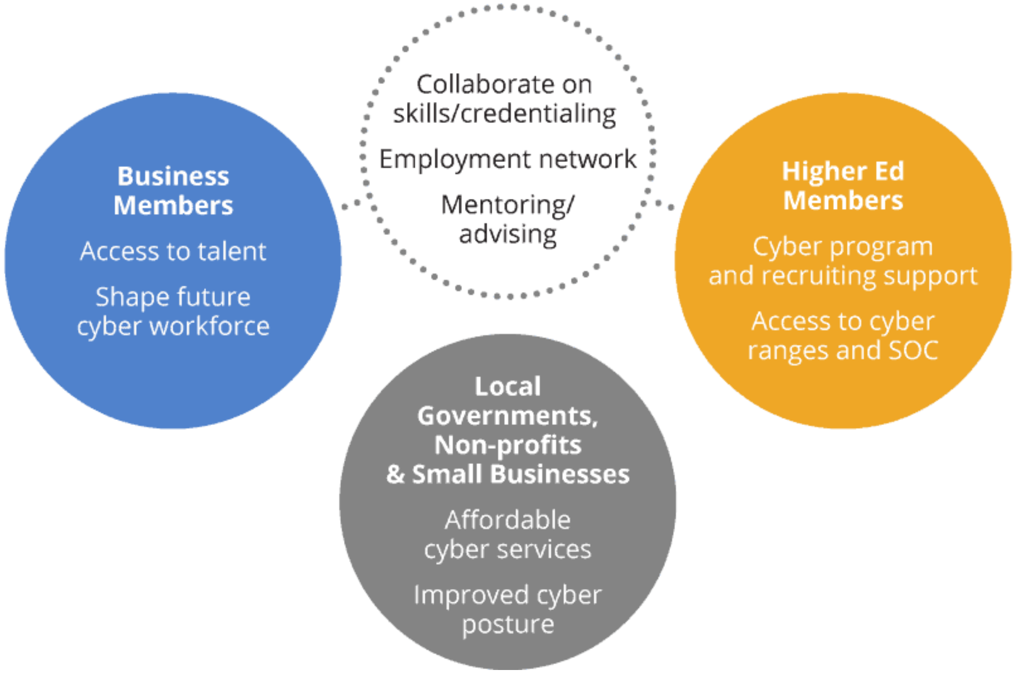
Percentage of SOC intern alumni placed in full time jobs within 3 months

4559

Students and Professionals Trained on Cyber Ranges

CyberTrust Massachusetts Consortium Overview

CyberTrust has formed a consortium of committed companies and colleges—anchored in community colleges and state universities, where programs can best reach underrepresented groups.



Collaborate on skills/credentialing
Employment network
Mentoring/ advising
Business Members
Access to talent
Shape future cyber workforce
Higher Ed Members
Cyber program and recruiting support
Access to cyber ranges and SOC
Local Governments, Non-profits & Small Businesses
Affordable cyber services
Improved cyber posture

Academic Members

BAY PATH UNIVERSITY 1897

BRIDGEWATER STATE UNIVERSITY

Cambridge College

ELMS COLLEGE

Franklin Cummings Tech

LASELL UNIVERSITY

MASSBAY COMMUNITY COLLEGE

PER SCHOLAS

Salem STATE UNIVERSITY

Simmons UNIVERSITY

STCC Springfield Technical Community College

UMass Boston

urbanleague of Eastern Massachusetts

UMASS LOWELL

Corporate Members

CISCO

MITRE

WEI

RAPID7

WOLF & COMPANY, P.C.

State-of-the-Art Cyber Ranges and SOCs Open in MA

BRIDGEWATER STATE UNIVERSITY

STCC Springfield Technical Community College

RAPID7

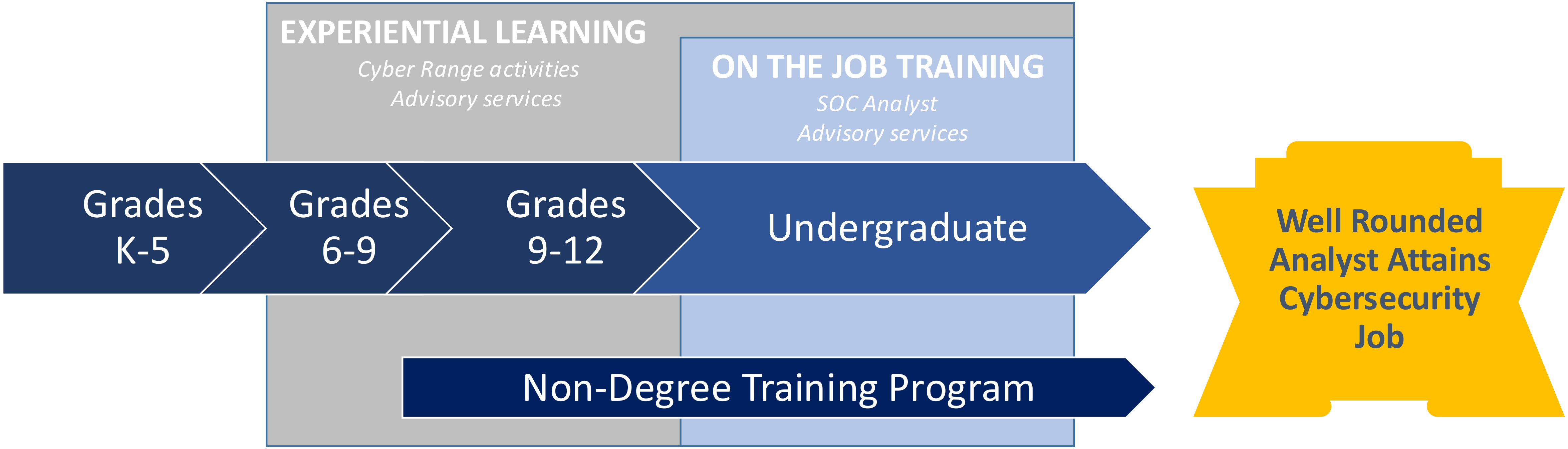
MASSBAY COMMUNITY COLLEGE

Salem STATE UNIVERSITY

Vision for a Massachusetts Cybersecurity Talent Pipeline

MassCyberCenter
at MassTech

A strong cybersecurity talent pipeline in Massachusetts would progress students through academic instruction or non-academic training programs and integrate experiential learning and on the job training.



EXPERIENTIAL LEARNING
Cyber Range activities
Advisory services
ON THE JOB TRAINING
SOC Analyst
Advisory services
Grades K-5
Grades 6-9
Grades 9-12
Undergraduate
Non-Degree Training Program
Well Rounded Analyst Attains Cybersecurity Job