Notice of Funding Opportunity for Cyber Resilient Massachusetts Grant Program Informational Webinar

*NOFO 2025-Cyber-01*

April 10, 2025

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	Resiliency for the Commonwealth (Public and Private Sector)	Communication, Collaboration, and Outreach
• Cybersecurity Training and Education Working Group • Jobs Board • Cybersecurity Mentorship Program • Cybersecurity SOC/Range • Alternative Cyber Career Education Grant Program	• Cyber Resilient Massachusetts Working Group • Tabletop exercises • Cyber Incident Response Plan Workshops • Resources for Municipalities • Cyber Resilient Massachusetts Grant Program	• Massachusetts Cybersecurity Month (October) • Citizen awareness • Ecosystem promotion • Talent recruitment • National cyber events • Webinars

MassCyberCenter at MassTech

CyberTrust Massachusetts: *The MassCyberCenter established this non-profit to deliver Security Operations Center (SOC) services to municipalities, small businesses, and non-profits across the Commonwealth with the support of student employees, as well as Cyber Range services to train students to enter the workforce and upskill professionals.*

SOC Range Program Outcomes To Date

- ➢ **2,314 students and professionals trained on Cyber Ranges**
- ➢ **31 entities received SOC services**
- ➢ **23 students employed as CyberTrust SOC employees**
- ➢ **70% of student employees found full-time cybersecurity employment with private or public organizations**
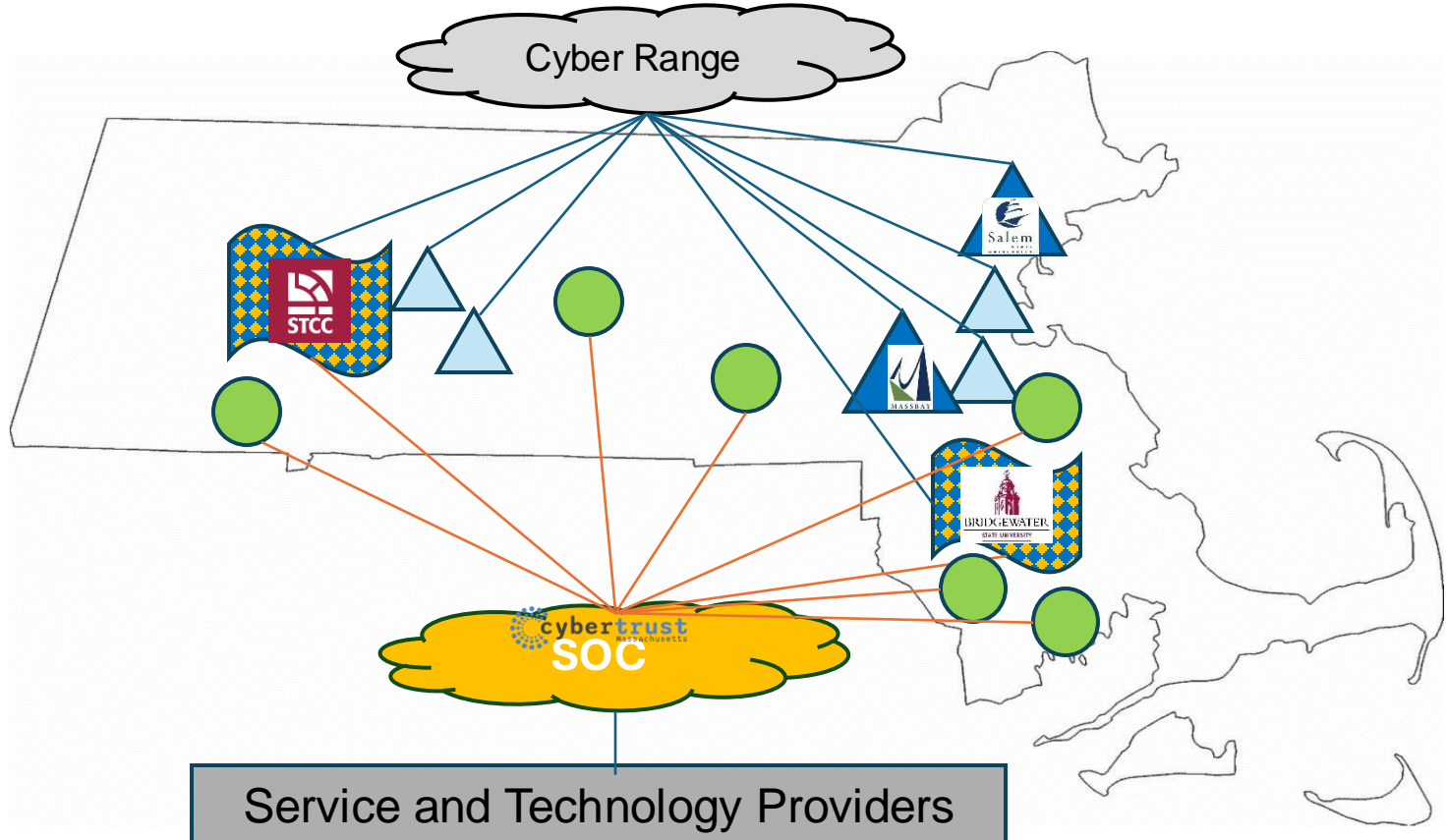
Legend

(flag icon)	Flagship SOC and Cyber Range (state-subsidized)
(dark triangle)	Mini Cyber Range (State-Subsidized)
(light triangle)	Mini Cyber Range (not State-Subsidized)
(green circle)	Municipality receiving SOC Services

Cyber Range

Service and Technology Providers

Updated Cyber Resilient Massachusetts Grant Program

Updated 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 and/or*== narrowly-focused cybersecurity technology upgrades identified through a cybersecurity vulnerability assessment.

Key Change: Municipal entities, small business, and non-profits are eligible to receive MDR from CyberTrust for up to 3 years

Additional Information

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

MassCyberCenter
at MassTech

Frequently Asked Questions

➢ **The cost of the scope of work for MDR I received from CyberTrust exceeds $25,000. Can I still apply for a grant?**

➢ **Is a match required for MDR projects?**

➢ **What is the timeframe of MDR grants?**

➢ **Can a municipality that has already received a grant under this program for a Technology Upgrade project apply for a grant for MDR?**

➢ **Can grants exceed $25,000 if multiple organizations receive MDR?**

➢ **Can a municipality already receiving MDR from CyberTrust apply for a grant?**

➢ **Is there a required start date for MDR projects?**

➢ **If I do not receive a grant during this application round, but still begin an MDR contract with CyberTrust, can I apply again utilizing the start date of the contract?**

MassCyberCenter
at MassTech
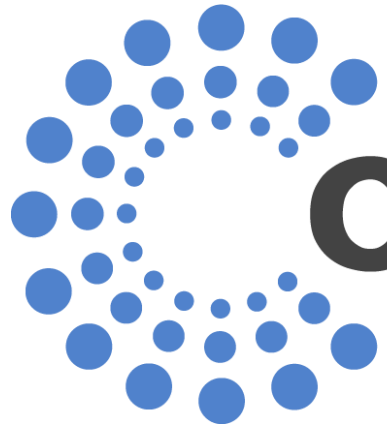
CyberTrust Managed Detection and Response

- Why CyberTrust?
  - CyberTrust is a security company—with deep security experience in Fortune 100, Defense/Intelligence and Global Consulting
  - Leveraging (and educating) a large team of student SOC analysts
  - Best-in-class tools and practices
- Why focus on Managed Endpoint Detection and Response?
  - Most attacks eventually pass through the endpoint
  - Top EDR vendors are current with the most advanced threats
  - Endpoint agents provide great visibility across the network
- Why SentinelOne?
  - Selected by CyberTrust in December 2023 for detection engine performance, ability to correlate events, and management capabilities
  - CyberTrust automation and service processes make the most of S1 capabilities

Comprehensive Protection Suite

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

PRICE:
    Municipal: $60

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

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*