Texas Education Agency

Cybersecurity Coordinator Forum

Todd Pauley, CISSP, CISM

Deputy CISO/Cybersecurity Coordinator

Texas Education Agency

todd.pauley@tea.texas.gov

August 23, 2023

Cybersecurity Coordinator Forum

The TEA **Information Security** team hosts a monthly meeting for **Texas LEA Cybersecurity Coordinators**, **ESC Cybersecurity personnel**, and other members of the community that support K12 Cybersecurity efforts. It provides content designed to assist LEAs and ESCs towards maturity in an information security program.

Register here with your LEA email address:

https://attendee.gotowebinar.com/register/8234183618339320587

Agenda

- Cybersecurity Announcements
  - TxISAO (Texas Information Sharing & Analysis Organization)
  - CISA Resources
  - State-Local Cybersecurity Grant Program (SLCGP)
  - CyberStart America
  - Cybersecurity Advisory
  - Updated Cybersecurity Incident Reporting
- Texas K-12 Cybersecurity Initiative
- Texas K12 Cybersecurity Program Preparation
  SentinelOne Offering Overview

TxISAO

ACTION: Please sign up for mailing list at the link below.

https://dir.texas.gov/txisao

The Texas Information Sharing & Analysis Organization (TxISAO) is open to all organizations in Texas to include K-12.

CISA – Cybersecurity for K-12 Education

K-12 Cybersecurity Tools and Resources

CISA worked with subject matter experts and K-12 working groups to customize this new webpage with tools and resources tailored for the K-12 community.

- Recommendations from their related report and CISA tools to help implement those recommendations.

- Links to free resources.
  - Including: FedVTE, Teacher and student cyber safety videos, etc.

https://www.cisa.gov/K12Cybersecurity

State and Local Cybersecurity Grant Program (SLCGP)

CISA Cybersecurity Grant

Texas was allocated approximately $40 million over four years. The allocation requires matching funds that increase through the years. (Note: Matching funds will be paid by grant sub-recipients.)

- The allocation is broken up into 4 years with awards happening individually in each year.
- A minimum of 80% of allocations must be passed through to local governments. In addition, at least 25% of the total funds made available under the grant must be passed through to rural communities.
- Requirements in order to be eligible:
  - Sign and participate in these free CISA services: Web Application Scanning, Vulnerability Scanning, Nationwide Cybersecurity Review (NCSR).
  - Join the TX-ISAO (free).

- Texas is submitting our Cybersecurity Plan for grant implementation. Once the plan has been accepted, proposals can be submitted and will be reimbursed if approved.

https://dir.texas.gov/information-security/state-and-local-cybersecurity-grant-program-slcgp

CyberStart America

CyberStart America Early Access

The National Cyber Scholarship Foundation (NCSF) is listening to teacher feedback and for the first time ever, CyberStart America is offering early access to the game starting THIS WEEK.

Teachers and students now have full access to the game, and students' points from last year will roll over. The official game launch is set for October 16th, 2023, but students will retain the points they earn starting now!

Important! Please use the following links to register:

Educator Registration - **https://register.cyberstartamerica.org/teacher/**

**PRO TIP: Don't forget to make your student groups before signing students up! You will save a lot of time if you have the group code ready to go at the time of registration then having to track them down later on.

(PDF Flyer available in the Handouts Section)

Student Registration -

https://register.cyberstartamerica.org/student/

**PRO TIP: Use the personalized referral link teachers received in their welcome email so your students auto-populate to your school. That will prevent them from accidentally registering for the wrong school due to typos and other issues.

Cybersecurity Advisories

CISA releases Malware Analysis Report on Barracuda Email Security Gateway Appliance (ESG) Vulnerability

- Various exploits creating backdoors:
  - Barracuda Exploit Payload and Backdoor
  - SEASPY
  - SUBMARINE
- IOC's available in the advisory linked below.
- Recommended actions are to contact Barracuda and swap out the device.

https://www.cisa.gov/news-events/alerts/2023/07/28/cisa-releases-malware-analysis-reports-barracuda-backdoors

Local Government Incident Reporting (SB 271)

Review

- SB 271 requires state agencies and local governments that experience a security incident to:
  - report to DIR within 48 hours after discovery (or to notify the secretary of state if the incident involves election data),
  - comply with the notification requirements of Section 521.053, Business & Commerce Code, to the same extent as a person who conducts business in this state, and
  - report to DIR the details of the security incident and an analysis of the cause of the incident within 10 days after incident eradication, closure and recovery.

- Effective September 1, 2023.

Local Government Incident Reporting (SB 271)

Definitions

Local government: a county, municipality, special district, school district, junior college district, or other **political subdivision of the state.**

Security incident:

- a breach or suspected breach of system security as defined by Section 521.053, Business & Commerce Code; and
- the introduction of ransomware, as defined by Section 33.023, Penal Code, into a computer, computer network, or computer system.

Local Government Incident Reporting (SB 271)

Process

- Incidents will be submitted using Archer Engage
- After creating an account, users can submit incidents and then the closure/post-mortem form
- This will replace the current School District Incident Report, required by Section 11.175 of the Education Code

https://dir.texas.gov/information-security/cybersecurity-incident-management-and-reporting/sb-271-security-incident

Texas Education Agency

Texas K12 Cybersecurity Initiative

June 2023

Texas K12 Cybersecurity Program Outreach

- **Building on and recapping the TAA published on June 15th:**
  - Request LEAs to take action to sign Inter-Local agreement with DIR prior to September 1, 2023.
  - Eligibility for fully funded Endpoint Detection and Response (EDR) includes LEAs with student enrollment of 15,000 or less. Licenses should be prioritized to highest risk devices (servers, central office staff and then others as needed), with a maximum limit of licenses equal to 10% of student enrollment.
  - Other cybersecurity services are on a first come first serve basis and will include Cybersecurity Assessments and Network Detection and Response (NDR).
  - TEA has created a webpage with up-to-date information as the program matures.
  - FAQs are in the process of being added to the site and should be up soon.

AT&T Security Consultants may be directly interacting with LEAs to help onboard to Managed Security Services with DIR. AT&T will also work closely with ESCs to assist with unified support to LEAs.

Grant for Cybersecurity Practitioners

Current recommendation based on feedback:

- Single grant awarded to one Region to centrally manage and coordinate best fit solutions for all regions.
- Grantee will distribute funds and help identify staffing solution for each region according to business need.
  - Direct hire, contract, interns, virtual, on-site, clustered team etc.
- Grantee will help facilitate uniform training, documentation, and team building opportunities for cybersecurity practitioners.
- Grantee will help facilitate resource sharing according to statewide needs and priorities.

Resources, Questions or Assistance?

Contact cybersecurity@tea.texas.gov

OR

Contact the Texas Department of Information Resources CISO Office at DIRSecurity@dir.texas.gov

TEA K-12 Cybersecurity Initiative Webpage

https://tea.texas.gov/academics/learning-support-and-programs/technology-planning/k-12-cybersecurity-initiative

Texas Education Agency

Texas K12 Cybersecurity Program
AT&T

Managed Security Services (MSS)

TEA-funded K-12 Cybersecurity Program

Gene Moore – 214.794.3149 gm4738@att.com

AT&T

August 22, 2023

Managed Security Services (MSS)

Overview & Eligibility

Meet the Team	**Kelly Alagna, Scott Kraeger, and Gene Moore Application Solutions Consultants, William (Bill) Higginbotham, Dir. of Cybersecurity Consulting, and Mark Willis, Principal Architect.**
Eligibility	**All ISD's and Public Charter Schools in the State of Texas** **EDR—Under 15K students/Staff & Admin 10% Security Assessments: All**
Must be Onboarded	**Must submit Customer Information Form (CIF) and be fully onboarded by DIR in order to participate.**
Timetable	**The program runs from September 1, 2023, through August 31, 2025.**
Services	**1) EDR—CrowdStrike or Sentinel 1—3 Flavors (Standard, Custom, EMA) 2)Security Control Assessments.**

Managed Security Services (MSS)

Onboarding

Complete the CIF	**Complete the Department of Information Resources (DIR) New Customer Information Form. Links provided by DIR and TEA. We can also send a hard copy if requested.**
DIR ILA/T&C's	**After receiving the CIF from the LEA, DIR will create and send the InterLocal Contract (ILC) and the Security T&C's to the LEA. The approval/signature of the ILC and the Security T&C'S will allow the LEA to participate in the State Shared Technology (STS) Program. The TEA program is part of the STS program.**
User Name and Password	**After DIR receipt, approval, and countersignature, the LEA will be set up with a Username/PW that will allow access to the STS portal. In the portal, the customer can now order services (After September 1, 2023).**
Order Received	**Once the order has been received and reviewed by MSI/DIR, the order will be forwarded to AT&T. AT&T will schedule a Service Verification Meeting (SVM). In the SVM with the LEA, we will discuss the order and validate the specific details for the delivery of service.**
Service Delivery	**After approval by the customer in the portal, the services will be delivered.**

Managed Security Services (MSS)

TEA-funded K-12 Cybersecurity Program

- **Program Dates: September 1, 2023 – August 31, 2025**
- **Funded Security Service Types:**
  - **Endpoint Detection Response (EDR) Service**
  - **Security Assessment (SA)**

Services are provided via the Texas Department of Information Resources (DIR) Shared Technology Services (STS) for K-12 and open-enrollment charter schools.

Endpoint Detection Response (EDR) Service

- **The EDR Service includes**:
  - Monitoring the health and performance of the EDR solution, resolving any health or performance issues of the EDR Monitoring platform
  - Monitoring the activity of the monitored devices when the endpoint is in communication with the EDR Management console
  - Installation of system updates, patches, and filters or definitions of the EDR platform
  - Performing and making configuration changes as required by the Customer
- **Target Audience:** Local education agencies (LEAs) with <15,000 students

Security Assessment (SA)

- **The SA scope includes security controls assessed in the following core areas**:
  - Review of business' information security program against the relevant National Institute of Standards & Technology and the Texas Cybersecurity Framework.
  - Full standardized security assessments of the general support systems for network, domain, server, endpoint, and email architectures.
  - Review of governance, processes, tools, and practices involving industry-specific technologies.
  - Review of industry-specific standards, guidelines, practices, and approaches considered against leading industry regulations.
- **Target Audience:** Any size LEA customer.

Managed Security Services (MSS)

Endpoint — Staff & Admin

What is Endpoint Security?

Endpoint Security is the process:	**of securing the various endpoints on a network, often defined as end-user devices.**
Devices include:	**Desktops, Laptops, Servers.** **Apple & Android. Mobile Devices including smartphones and tablets.**
Operating Systems Supported:	**Windows, Linux, Unix, MacOS, iOS, Android.**
Endpoints serve as:	**Points of access to an enterprise network and create points of entry that can be exploited by malicious actors.**
Endpoint security software protects:	**The points of entry from risky activity and/or malicious attack.**

Managed Security Services (MSS)

TEA/MSS Available EDR Service Options

Standard

- MSS security professionals monitor and manage your EDR solution.
- MSS actively looks for threats, indicators of compromise (IoC's) and malware.
- MSS provides response actions and/or alerts when an endpoint device may be compromised.
- Read-only access to EDR console.

Custom

- Solution is 100% customer/vendor-managed. AT&T does not manage
- DIR provides monitoring and alerting.
- Customer will provide EDR events (via syslog) to the MSS shared services SIEM.
- MSS cross-correlates events against other state-wide event data & provides alerts and notifications to customers.
- Customer should have a SOC in place to be approved for this option.

Endpoint Monitoring and Alerting (EMA)

- Customer continues to use their current EDR solution.
- Customer will provide EDR events (via syslog) to the MSS shared services SIEM.
- MSS cross-correlates events against other state-wide event data & provides alerts and notifications to customers.
- Utilizes an existing deployed endpoint solution.
- MS Defender, CarbonBlack, SentinelOne, CrowdStrike, Insight IDR, Cynet, Checkpoint, F-Secure, Cortex XDR, ApexOne.

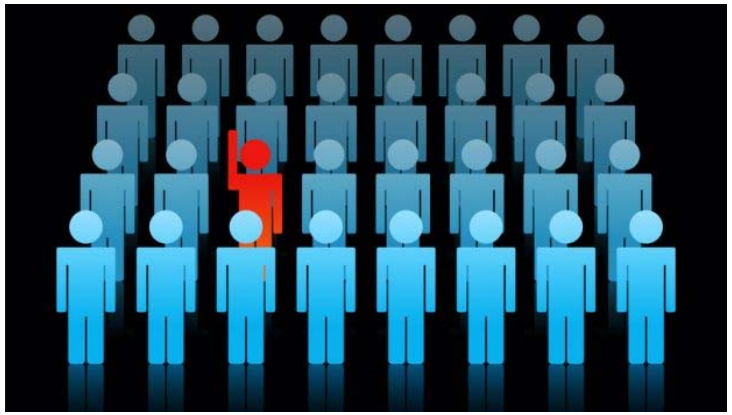
Managed Security Services (MSS)

Endpoint Detection Response (EDR) Service

Benefits of the EDR Service

- Protects the customer's endpoint devices across multiple platforms (Windows, MacOS, and Linux).
- Manage, detect, and respond 24/7 to near real-time threats and suspicious events including malware and ransomware.
- Multiple EDR service options are available to LEAs that incorporate existing technology solutions through this program.

Underlying technologies based on customer preferences (CrowdStrike or Sentinel One driven).



Is your threat monitoring and response strategy mission-ready?

This Photo by Unknown Author is licensed under CC BY-SA-NC

Managed Security Services (MSS)

TEA/MSS Endpoint Detection and Response (EDR)

EDR Solution Benefits

- Deployment Support Services
  - Provides support during the planning & deployment phases.
  - Provides EDR policy and configuration recommendations.
- Consumption-based billing w/ no term commitment
  - Only billed for active end-points per month.
  - Priced with state-wide volume tier discounts.
- Aggregated State threat data
  - Unique event correlation & insights leveraging all State of Texas shared network data traffic at the DIR NSOC.
  - Allows for proactive blacklisting and protection for all endpoints across all MSS EDR customers.
  - Fully-managed via Next-Gen SIEM monitoring.
- TxRamp compliance in place.

Additional EDR Operational Benefits

- Customized based on organizational needs.
- Real-time threat detection & response for all alerts.
- 24x7 monitoring and alerting by MSS analysts.
- Turn-key Program: Plan, Design, Deploy, Manage.
- Over 120,000 End-points are protected under MSS EDR already.
- On-going Management, reviews, and detailed reporting.
- SLA protections built into the DIR-MSS contract.
- AT&T one of the largest MSSP's in the world
- Direct ordering via State of Texas Managed Security Services Contract: DIR-MSS-SCP-001.
- No RFP required.

Managed Security Services (MSS)

TEA-funded K-12 Cybersecurity Program

- **Program Dates: September 1, 2023 – August 31, 2025**
- **Funded Security Service Types:**
  - **Endpoint Detection Response (EDR) Service**
  - **Security Assessment (SA)**

Services are provided via the Texas Department of Information Resources (DIR) Shared Technology Services (STS) for K-12 and open-enrollment charter schools.

Endpoint Detection Response (EDR) Service

- **The EDR Service includes**:
  - Monitoring the health and performance of the EDR solution, resolving any health or performance issues of the EDR Monitoring platform
  - Monitoring the activity of the monitored devices when the endpoint is in communication with the EDR Management console
  - Installation of system updates, patches, and filters or definitions of the EDR platform
  - Performing and making configuration changes as required by the Customer
- **Target Audience:** Local education agencies (LEAs) with <15,000 students

Security Assessment (SA)

- **The SA scope includes security controls assessed in the following core areas**:
  - Review of business' information security program against the relevant National Institute of Standards & Technology and the Texas Cybersecurity Framework.
  - Full standardized security assessments of the general support systems for network, domain, server, endpoint, and email architectures.
  - Review of governance, processes, tools, and practices involving industry-specific technologies.
  - Review of industry-specific standards, guidelines, practices, and approaches considered against leading industry regulations.
- **Target Audience:** Any size LEA customer.

Managed Security Services (MSS)

Security Assessment

Benefits of a Security Assessments

- Comprehensive third-party reviews of business' information security program.
- DIR–approved Security Score Baseline and Detailed Security Reporting provided.
- Scorecard summarizes Security Program's Maturity correlated to State Averages by Size and Scope metrics.
- Provides precise and clear communication vehicle to inform leadership decision-making including operational, technical and non-technical resource alignment.

Areas of Strength and Issues of Opportunity discovery with recommended guidelines.

This Photo by Unknown Author is licensed under CC BY-NC-ND

Managed Security Services (MSS)

DIR Special Program

TEXAS DIR
Shared Technology Services

TEA
Texas Education Agency

Technology Alliance for Statewide Initiatives

AT&T

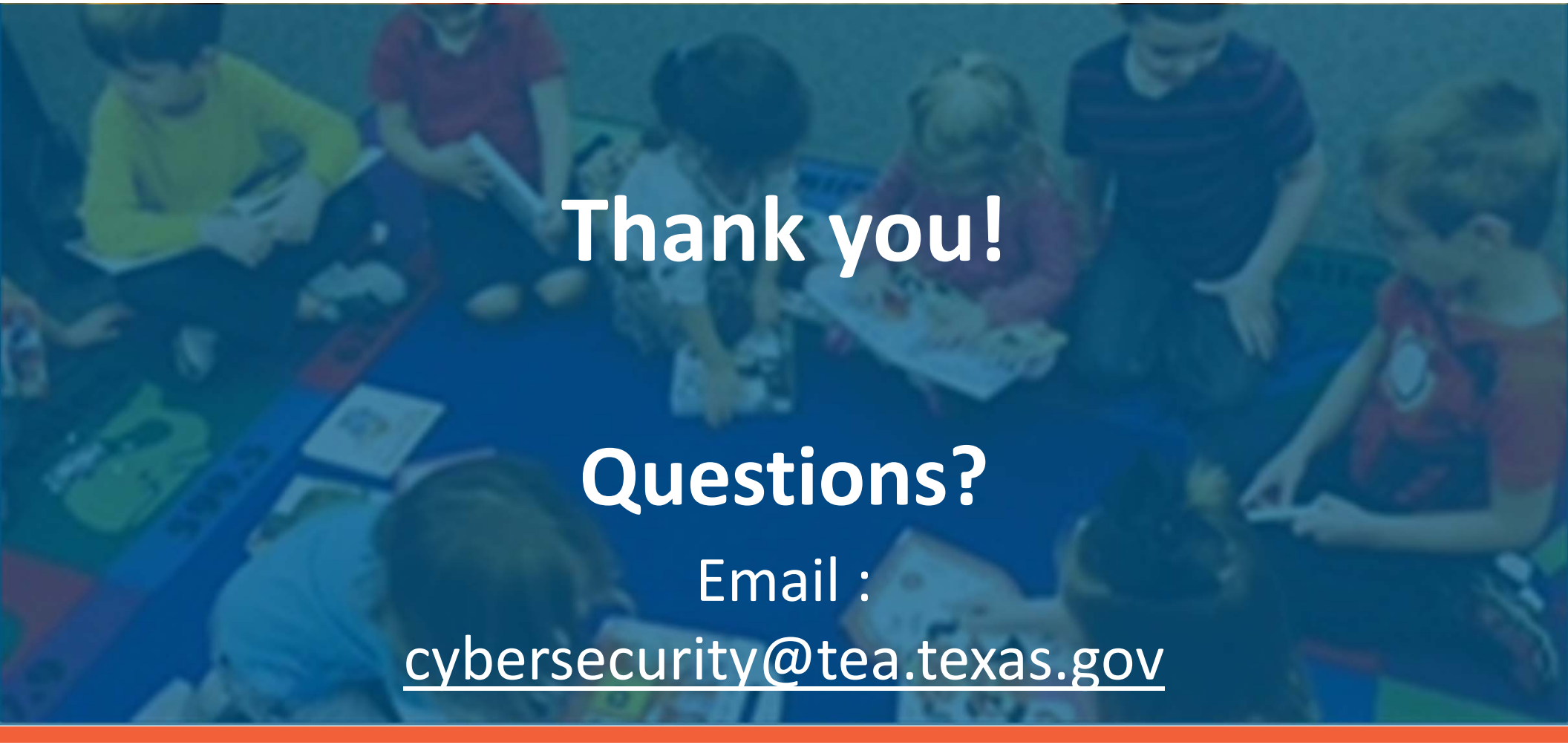
SentinelOne

CROWDSTRIKE

This offering represents a partnership between DIR, TEA, TASI (Technology Alliance for Statewide Initiatives), as well as select STS MSS Providers.

Thank You!!

Gene Moore gm4738@att.com 214-794-3149
Scott Kraeger sk7415@att.com 916-402-6378
Kelly Alagna ka210m@att.com 469-786-9468



Thank you!

Questions?

Email :
cybersecurity@tea.texas.gov