TEA
Texas Education Agency

Cybersecurity Coordinator Forum

Todd Pauley, CISSP

Deputy CISO/Cybersecurity Coordinator

Texas Education Agency

todd.pauley@tea.texas.gov

May 24, 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)
  - Cybersecurity Advisories
- Legislative Updates
- Dorkbot
  - Cam Beasley UT – Austin, CISO
- Texas K12 Cybersecurity Program Preparation

  CrowdStrike Offering Overview

TxISAO

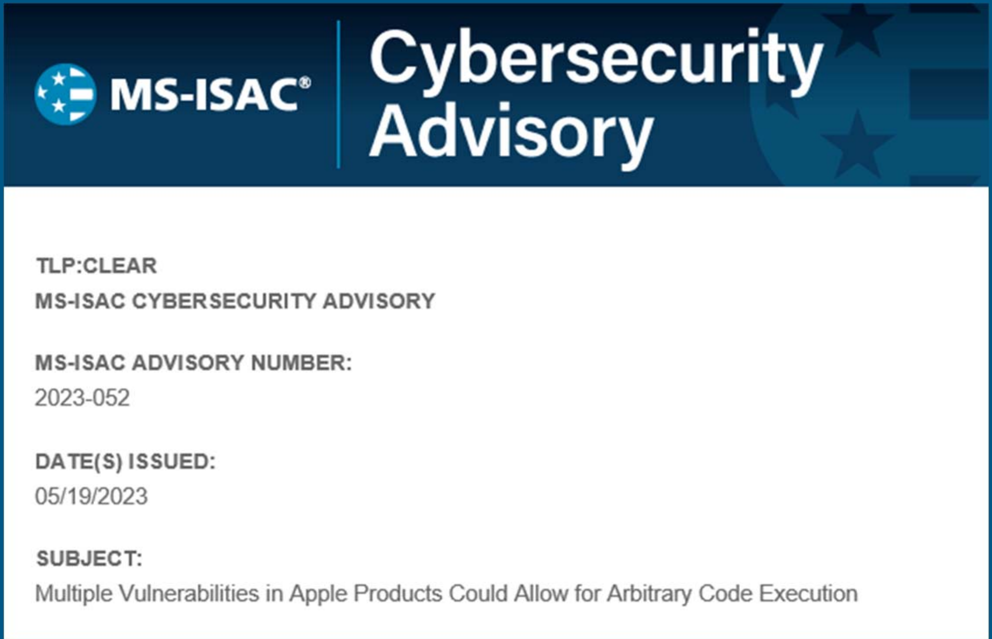
ACTION: Please sign up for mailing list at the link below.

https://dir.texas.gov/txisao

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

Cybersecurity Advisories

Apple Vulnerabilities



TLP:CLEAR
MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER:
2023-052

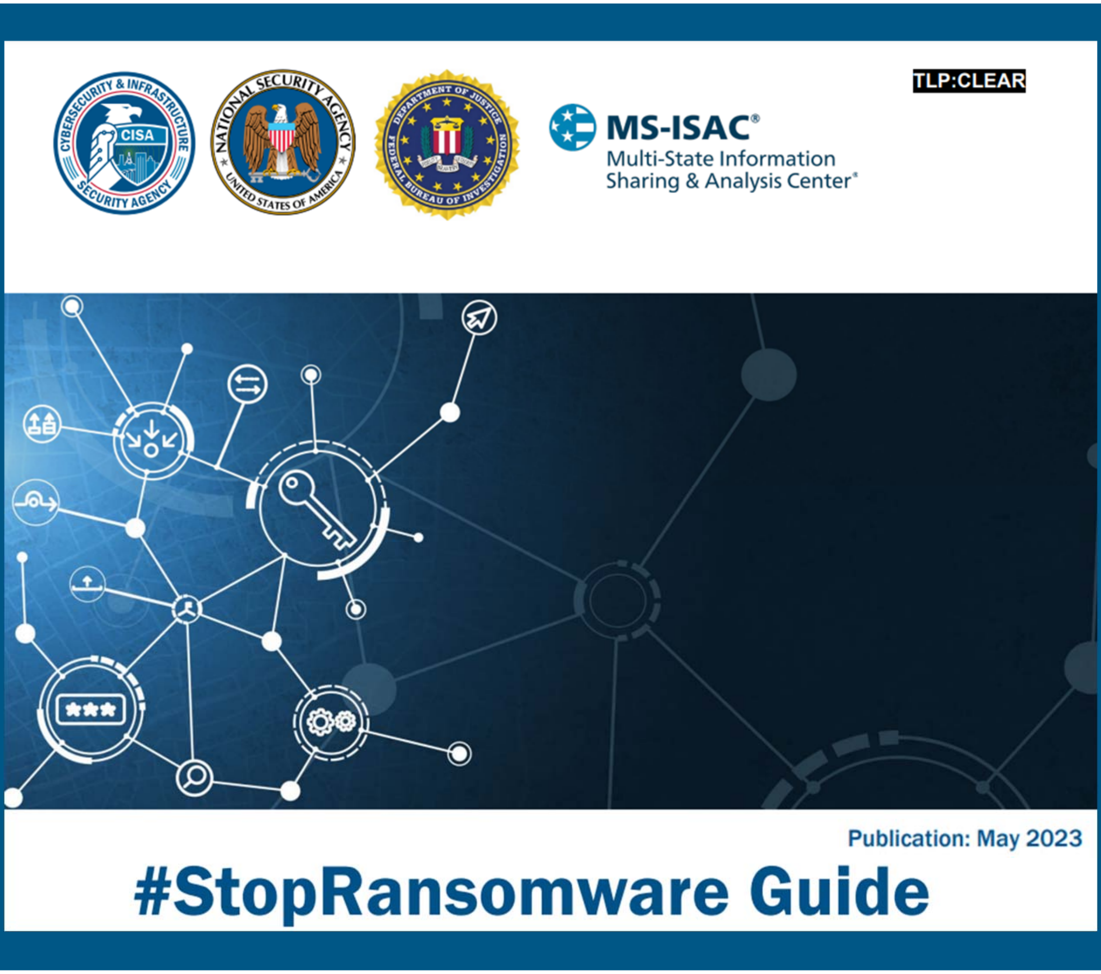
DATE(S) ISSUED:
05/19/2023

SUBJECT:
Multiple Vulnerabilities in Apple Products Could Allow for Arbitrary Code Execution

https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-apple-products-could-allow-for-arbitrary-code-execution_2023-052

Texas Education Agency

CISA’s Stop Ransomware Guide



TLP:CLEAR

MS-ISAC®
Multi-State Information
Sharing & Analysis Center®

Publication: May 2023

#StopRansomware Guide

- Originally released in 2020.
- The update incorporates lessons learned from the past two years and includes additional recommended actions, resources, and tools to maximize its relevancy and effectiveness and to further help reduce the prevalence and impacts of ransomware.

https://stopransomware.gov

TEA
Texas Education Agency

Legislative Updates

Legislative Updates

88th Legislative Session

140 days of lawmaking

- Jan. 10th : The regular session of the 88th Texas Legislature convened.
- March 10th : Deadline to propose any additional bills to the already 1,600 amassed before the session began.
- May 29th : Session adjournment (sine die).
- June 18th : Post-session deadline for the governor to sign or veto legislation.
- September 1st : Date most passed bills take effect (FY 2024).
- DIR's Cybersecurity Bill Tracking: https://dir.texas.gov/technology-legislation?id=31

Signed by the Governor.

Takes effect September 1, 2023

SB 271

Local Governments Security Incident Procedures

- Updates Government Code 2054.1125 to include local governments in reporting requirements that previously only applied to state agencies.
- Notify DIR and State of Texas CISO within 48 hours of discovery and detailed account within 10 days after eradication.

“Security incident” means:

(A) breach or suspected breach of system security as defined by Section 521.053, Business & Commerce Code:

> *the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data.*

(B) the introduction of ransomware, as defined by Section 33.023, Penal Code, into a computer, computer network, or computer system.

Texas Education Agency

Legislative Updates

Passed both houses.
Sent to the Governor.

Takes effect September 1, 2023

SB 768

Reporting Data Breach Information to the Attorney General

Reporting on data breaches involving 250 Texans:

- Changes timeframe from 60 days to as soon as practicable but no later than 30 days after discovery.

Legislative Updates

A version has passed both houses. Differences include whether this would apply to Local Governments or just State Agencies. Differences will be worked out in conference committees.

SB 1893

Relating to prohibiting the use of certain social media applications and services on devices owned or leased by governmental entities.

- Would ban TikTok and any other applications my by its parent company, ByteDance.
- Would ban any applications declared by executive order of the governor.

Purpose of Texas K12 Cybersecurity Program

- Immediate solutions to protect Local Education Agencies (LEAs) from major cyber incidents until LEAs can transition to the State funded Regional Security Operation Centers (RSOCs) and get full service.
- Priority will be given to rural LEAs
- Priority is to get Endpoint Detection and Response (EDR) onboarded and operational to as many LEAs as possible.
- Cybersecurity assessments will provide baseline of the cybersecurity maturity of LEAs.
- Network Detection and Response (NDR) for schools with cameras and other Internet of Things (IoT) devices.
- Cybersecurity practitioners will assist with implementation.

Preparation for Texas K12 Cybersecurity Program

In anticipation of the

TEA Cybersecurity Program

launch next fiscal year, we would like LEAs positioned to be able to receive security services as soon as possible.

Based on current planning:

- **Managed Security Service (MSS)** from Department of Information Resources (DIR)
- **Provide select security services**
- **Free of charge for LEAs**

Dorkbot

Cam Beasley, CISO

University of Texas at Ausitn

UT Cybersecurity Services for K-12 Education

INFORMATION SECURITY OFFICE
UNIVERSITY OF TEXAS
AT AUSTIN
SECURUS * VIGILARE * INSANUS

Cam Beasley – CISO | UT Austin | cam@utexas.edu

Overview of Cybersecurity Efforts/Offerings

Dorkbot :: Managed Web Vulnerability Detection & Response

A no-cost automated security service extended to ISDs throughout the state of Texas.

Sign-up form: https://security.utexas.edu/dorkbot

Dorkbot :: Managed Web Vulnerability Detection & Response

Automatically Identifies Serious Web Vulnerabilities

Dorkbot has proven valuable in defending organizations from data exfiltration and other attacks targeting exposed web applications.

Subscribers since Mar 2017
2,400+ Entities Served across
205 countries
97% of R1s, 99% of R2s/R3s,
100% of Tribal Colleges & HBCUs

200,000+ Verified Vulns

- SQL injection,
- Cross-site Scripting,
- LFI, RFI, OSi, LDAPi

99% of Texas Universities / Colleges Covered

INFORMATION SECURITY OFFICE
SECURUS ✶ VIGILARE ✶ INSANUS

Dorkbot :: Some Key Service Details

1. All notifications will source from security@utexas.edu.
2. All Dorkbot checks will come from autoscan.infosec.utexas.edu (146.6.15.11). We encourage organizations to create an exception for this systems to ensure we can scan pages.
3. We also use the following User-Agent string so that you can easily spot us in your web logs: **UT-Dorkbot/1.2.**
4. We can also exclude targets from the service as needed, by: IP address, host name, subdomain or regex string in a URL.
5. We will also provide you with automated monthly summary report of Dorkbot's activity for your organization if we report any findings in that month.

INFORMATION SECURITY OFFICE
SECURUS * VIGILARE * INSANUS

Dorkbot :: How does it work?

1) Dorkbot doesn’t crawl sites, but it does query the latest public internet crawl data. e.g., Internet Archive (https://archive.org) and CommonCrawl (https://commoncrawl.org). We're looking for likely-dynamic pages since they're the highest risk, so we specifically ask for all the links that contain a question mark followed by parameters, which guarantees that there are inputs for us to probe for vulnerabilities. These are Dorkbot’s initial targets.

2) Dorkbot filters the targets through a blocklist of hosts and keywords that our subscribers have requested exclusions for. Things like under-resourced servers that have long-running page requests, or login forms that generate emails for every failed attempt, etc.

3) Then we generate a unique representative list of what's left by discarding any pages that are too similar to others already in the list, in order to maximize our resource usage and scan as many disparate targets as we can for the organizations we serve.

NOTE: If a page isn’t public, it won’t be evaluated by Dorkbot.

Dorkbot :: Managed Web Vulnerability Detection & Response

Additional Background
https://er.educause.edu/blogs/2019/2/dorkbot-a-managed-application-security-assessment-service-for-higher-education

https://www.statesman.com/story/business/technology/2019/05/17/uts-security-team-takes-google-hacking-service-global/5110348007/

INFORMATION SECURITY OFFICE

UNIVERSITY OF TEXAS AT AUSTIN

SECURUS * VIGILARE * INSANUS

security@utexas.edu

Texas Education Agency

Texas K12 Cybersecurity Program CrowdStrike

CROWDSTRIKE

TEA-DIR-AT&T-CROWDSTRIKE

Tracey Mills- VP Public Sector in North America
Parker Anderson– Regional Account Manager- Texas K-12

CROWDSTRIKE

AGENDA

- Who is CrowdStrike
- Falcon EDR
- TEA-AT&T-DIR Offer
- AT&T Onboarding and Management
- Q&A, Next Steps

RANKED #1 IN EDR, EPP & XDR BY OUR CUSTOMERS

Gartner peerinsights customers' choice™

Gartner Peer Insights

- 4.9/5 in EDR with 314 reviews
- 4.8/5 in Endpoint Protection Platforms with 837 reviews
- 4.8/5 overall with 1280 reviews

G2 Leader WINTER 2023

G2

- #1 in EDR (Enterprise, Mid-Market, Overall)
- #1 XDR (Enterprise, Overall)
- #1 in Threat Intelligence, and Ent Antivirus
- Earned G2 Leader Badges across 16 categories
- 207 Reviews, 4.7 Star Rating

TrustRadius ★ TOP RATED 2022

TrustRadius

- Won Top Rated Award for EPP and XDR
- Received additional Top Rated Awards for -- Antivirus, Cloud Computing Security, Incident Response, Intrusion Detection, MDR, Threat Intelligence, Vulnerability Management
- 132 reviews, 9.1 out of 10

PeerSpot No.1 Ranked ★★★

PeerSpot

- #1 Ranked Badge in EDR
- #1 Ranked Badge in MDR, Anti-Malware, Threat Intelligence Platforms
- Gold Peer Awards in EPP and EDR
- 50 Reviews, 4.5 out of 5

TESTED & VALIDATED BY ALL MAJOR THIRD-PARTY FIRMS

MITRE

Highest Detection Coverage

99% detection coverage in the 2022 MITRE Engenuity ATT&CK® Evaluations for Security Service Providers

SE Labs

100% Ransomware Prevention

100% protection with zero false positives in SE Labs Enterprise Advanced Security Ransomware Test

IDC

#1 in Endpoint Security Market Share

Highest market share of all providers for both Corporate & Modern Endpoint Security

FROST & SULLIVAN

Leader in Cloud Security & Threat Intelligence

Named a Leader in Frost & Sullivan's 2022 Cloud-Native Application Protection Platform and Frost Radar™: Global Cyber Threat Intelligence report

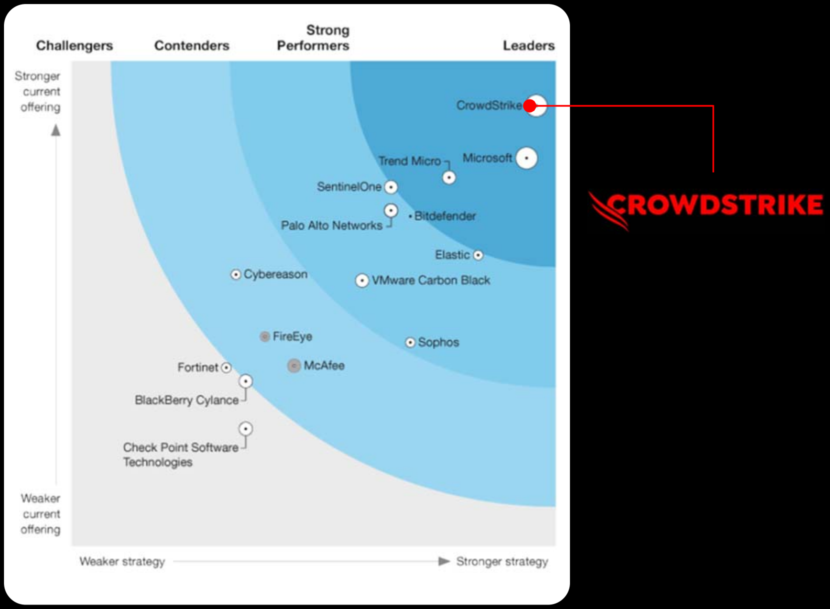
CROWDSTRIKE

THIRD CONSECUTIVE TIME AS A LEADER

A LEADER IN FORRESTER'S ENDPOINT DETECTION & RESPONSE WAVE

FORRESTER®

CROWDSTRIKE DOMINATES IN EDR WHILE BUILDING ITS FUTURE IN XDR AND ZERO TRUST.



The Forrester Wave™:
Endpoint Detection And Response Providers, Q2 2022, April 6, 2022

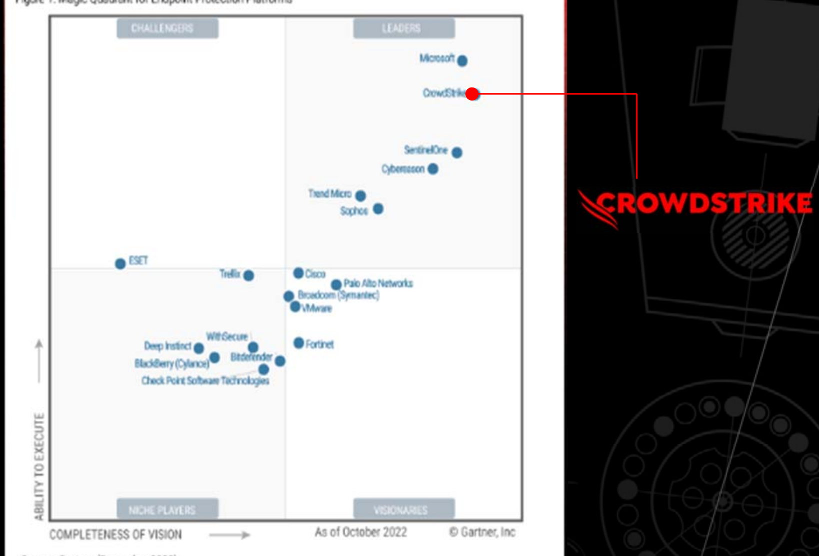
SECOND CONSECUTIVE TIME AS A LEADER

A LEADER IN GARTNER'S ENDPOINT PROTECTION PLATFORMS MAGIC QUADRANT

Gartner.

POSITIONED FURTHEST FOR COMPLETENESS OF VISION

Figure 1: Magic Quadrant for Endpoint Protection Platforms



Source: Gartner (December 2022)

Gartner Magic Quadrant for Endpoint Protection Platforms, Paul Webber, Peter Firstbrook, Rob Smith, Mark Harris, Prateek Bhajanka,5th May 2021. This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from CrowdStrike. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

CROWDSTRIKE

Highest Detection Coverage

MITRE ENGENUITY
ATT&CK® EVALUATIONS
Managed Services
OilRig
PARTICIPANT
2022

- ✓ The only vendor with 75/76 steps covered
- ✓ 2022 MITRE Engenuity ATT&CK® Evaluations for Security Service Providers

CROWDSTRIKE

CUSTOMER QUOTES

- “CrowdStrike saved our a**. Had we not been told of an attack at 10PM on a Friday night, our school District would have been owned and we would all be looking for new jobs. Everyone, even the sales Team was quick to engage and help understand the scenario and remediate as quickly as possible.”- CIO of Central Texas ISD

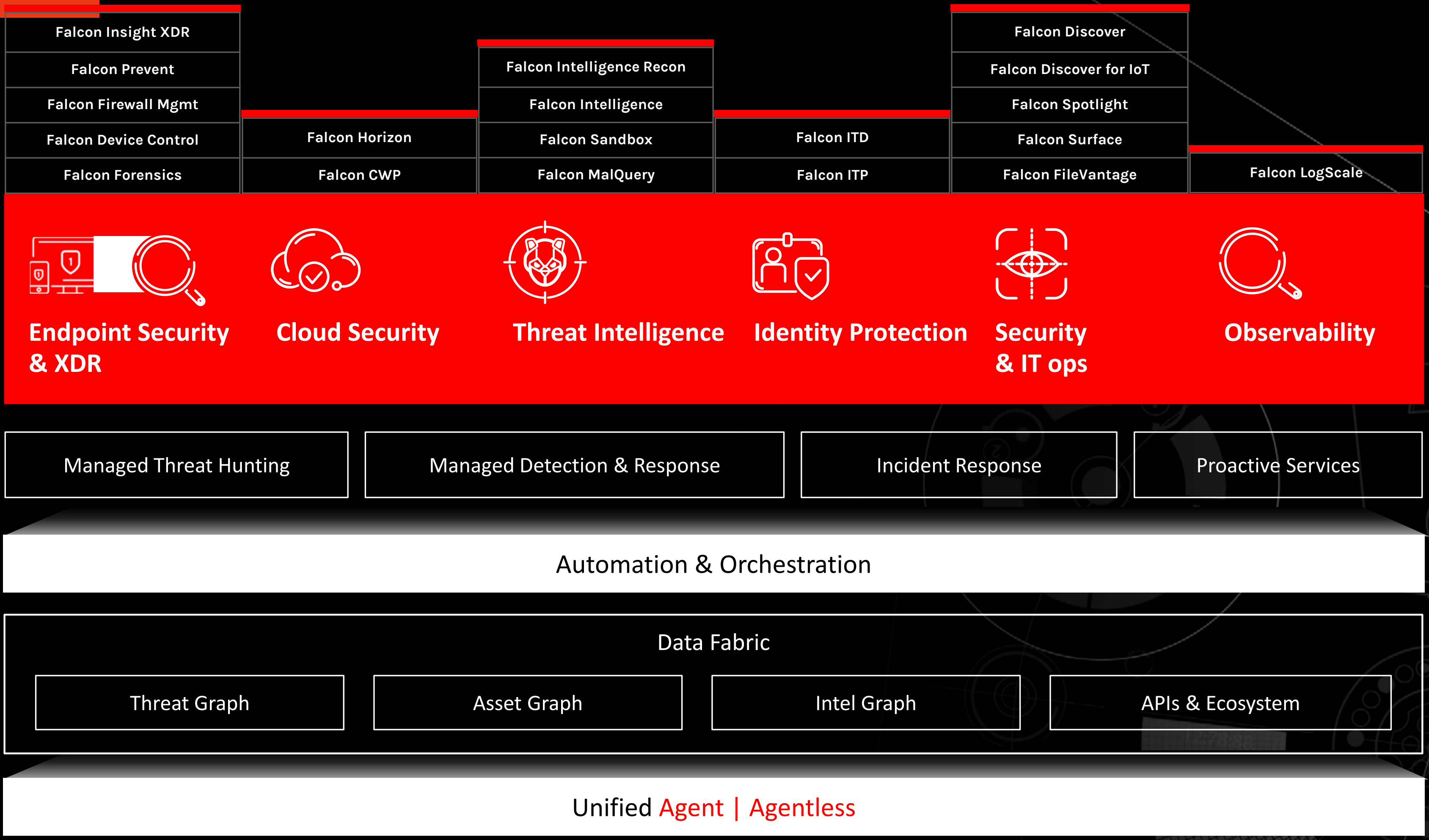
- ”During a very chaotic 24-48 hours, we were just trying to get our arms around what was happening, Reaching out to CrowdStrike ended up being our saving grace.”- Jason Rooks, CIO of Parkway School District

[Deploying the competitors agent was] “not as smooth, the agent was not as lightweight, more significant
Impact on the endpoints, we saw a negative impact when we went to deploy to our data center.” – Jason Rooks, CIO of Parkway School District

“My team and I sleep better at night knowing that CrowdStrike and the Complete team are monitoring our environment.” - Jason Rooks, CIO of Parkway School District

“What’s incredible to me is how incredible we get a call.” “Teacher installs something they shouldn’t, we get that call. The process works. Its fast, its streamlined. Thats why we are happy CrowdStrike

CROWDSTRIKE



Endpoint Security & XDR

- Falcon Insight XDR
- Falcon Prevent
- Falcon Firewall Mgmt
- Falcon Device Control
- Falcon Forensics

Cloud Security

- Falcon Horizon
- Falcon CWP

Threat Intelligence

- Falcon Intelligence Recon
- Falcon Intelligence
- Falcon Sandbox
- Falcon MalQuery

Identity Protection

- Falcon ITD
- Falcon ITP

Security & IT ops

- Falcon Discover
- Falcon Discover for IoT
- Falcon Spotlight
- Falcon Surface
- Falcon FileVantage

Observability

- Falcon LogScale

Managed Threat Hunting | Managed Detection & Response | Incident Response | Proactive Services

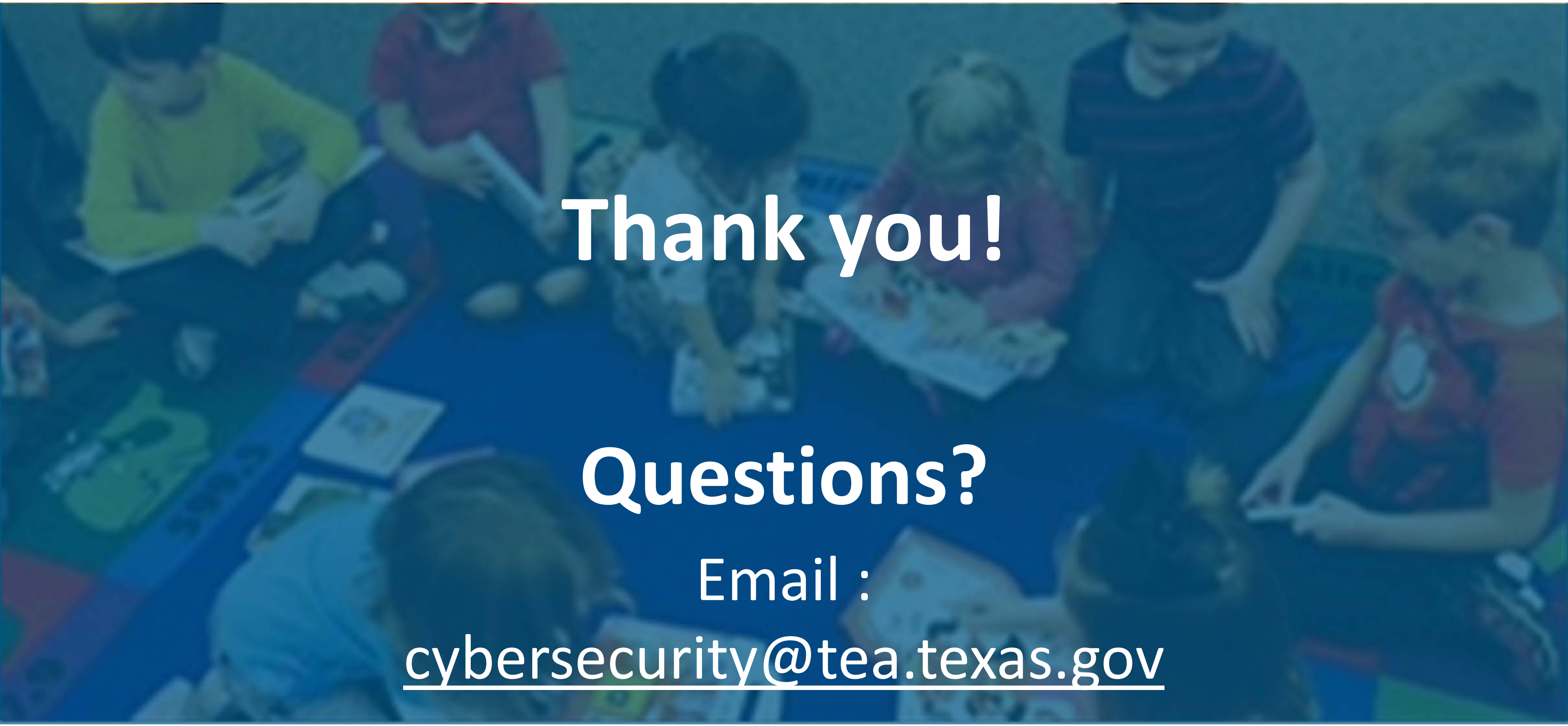
Automation & Orchestration

Data Fabric

Threat Graph | Asset Graph | Intel Graph | APIs & Ecosystem

Unified Agent | Agentless

AT&T



Thank you!

Questions?

Email :

cybersecurity@tea.texas.gov