



Cybersecurity Coordinator Forum

Todd Pauley, CISSP
Deputy CISO/Cybersecurity Coordinator
Texas Education Agency
todd.pauley@tea.texas.gov



June 28, 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
- 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>

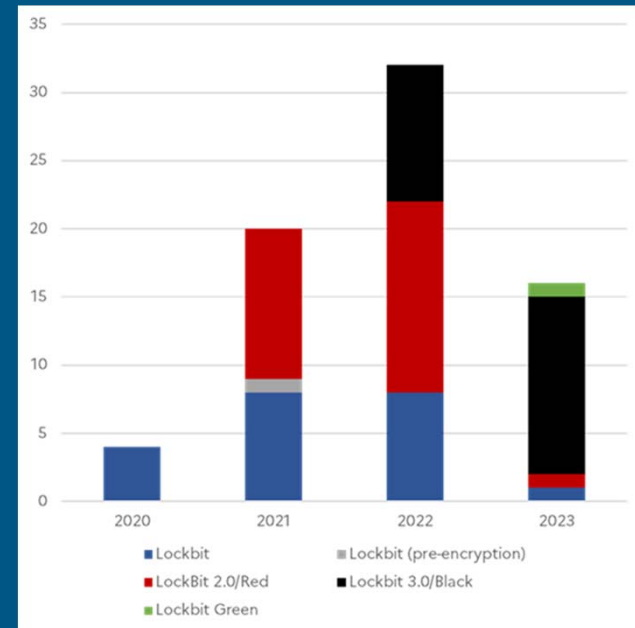


The Texas Information Sharing & Analysis Organization (TxISAO)
is open to all organizations in Texas to include K-12.

CISA and Partners Release Joint Advisory on Understanding Ransomware Threat Actors: LockBit

TLP: Clear

- In 2022, LockBit was the most deployed ransomware variant across the world and continues to be prolific in 2023.
- LockBit ransomware functions as a Ransomware-as-a-Service (RaaS) model where affiliates are recruited to conduct ransomware attacks using LockBit ransomware tools and infrastructure.
- Approximately \$91M U.S. ransoms paid since LockBit activity was first observed in the U.S. on January 5, 2020 (approx. 1,700 attacks).



<https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a>



Cybersecurity Advisories

CISA and Partners Release Joint Advisory on Understanding Ransomware Threat Actors: LockBit

TLP: Clear

Common Vulnerabilities and Exposures (CVEs) Exploited:

- CVE-2023-0669: Fortra GoAnywhere Managed File Transfer (MFT) Remote Code Execution Vulnerability
- CVE-2023-27350: PaperCut MF/NG Improper Access Control Vulnerability
- CVE-2021-44228: Apache Log4j2 Remote Code Execution Vulnerability,
- CVE-2021-22986: F5 BIG-IP and BIG-IQ Centralized Management iControl REST Remote Code Execution Vulnerability,
- CVE-2020-1472: NetLogon Privilege Escalation Vulnerability,
- CVE-2019-0708: Microsoft Remote Desktop Services Remote Code Execution Vulnerability, CVE-2018-13379: Fortinet FortiOS Secure Sockets Layer (SSL) Virtual Private Network (VPN) Path Traversal Vulnerability.

<https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a>





Cybersecurity Advisories

CISA and FBI Release #StopRansomware: CLOP Ransomware Gang Exploits MOVEit Vulnerability

TLP: Clear

Beginning on May 27, 2023, CLOP Ransomware Gang, also known as TA505, began exploiting a previously unknown SQL injection vulnerability (CVE-2023-34362) in Progress Software's managed file transfer (MFT) solution known as MOVEit Transfer.

This vulnerability is remediated in the most current version of MOVEit.

Other mitigating factors and IOCs are listed in the advisory at the link below.

<https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a>



An aerial photograph of Austin, Texas, showing the city skyline with various skyscrapers and buildings. The Colorado River flows through the city, with a bridge crossing it. The scene is captured during the golden hour, with warm sunlight reflecting off the buildings and the water. A semi-transparent white banner is overlaid across the middle of the image, containing the text "Legislative Updates".

Legislative Updates

The Texas Legislature typically files about 1,000 education-related bills every session

1,474 Education Bills filed this session

- **50** Hearings on Education Related Bills
- **127** Bills Heard in House Public Education Committee
- **160** Bills Heard in Senate Education Committee
- **141** Passed both Chambers and became law



This presentation provides a synopsis of 18 of the 141 education bills passed.



HB 4553 DIR Services Eligibility:

- Clarifies rules regarding who may utilize DIR's services.
- Allows an agency to pay for services for an eligible entity.
- Open enrollment charter schools included.

SB 271 Local Governments Cybersecurity Incident Reporting:

- Updates Government Code 2054.1125 to include LEAs in reporting requirements.
- Broadens requirements from student PII under TEC 11.175, to any **suspected** breach of information.
- Notify DIR and State of Texas CISO within 48 hours of discovery and detailed account within 10 days after eradication.
- Specifically lists ransomware as needing to be reported to DIR.

*For more information and updates on SB 10 please visit: <https://www.trs.texas.gov/Pages/benefit-enhancements-2023.aspx>



SB 768 Reporting Breaches 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.

SB 1893 Prohibiting TikTok and other security risky applications:

- Bans TikTok and any other applications my by its parent company, ByteDance and any other application deemed to be a security risk by the governor.
- School districts are included in the definition of governmental entities.
- Mirrors the Executive Order issued by the governor last fall for state agencies.
- A governmental entity shall adopt a policy prohibiting the installation or use.

*For more information and updates on SB 10 please visit: <https://www.trs.texas.gov/Pages/benefit-enhancements-2023.aspx>



HB 18 Protection of minors on digital services and devices:

- Requires users to register with their age for a digital services and social media.
- Minors will need parental consent.
- Reduce marketing content to minors
- TEA shall adopt standards for permissible electronic devices and software used by a school district.
- When issuing a device, LEAs must “install an Internet filter that blocks and prohibits pornographic or obscene materials or applications, including from unsolicited pop-ups, installations, and downloads.”
- Establishes a joint committee of the legislature to study the effects of media on minors.

*For more information and updates on SB 10 please visit: <https://www.trs.texas.gov/Pages/benefit-enhancements-2023.aspx>



Texas K12 Cybersecurity Initiative

June 2023



Texas K12 Cybersecurity Program Outreach

- **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. Initial distribution will only be available for servers and staff, 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:
- **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.**



Dorkbot – Web Application Vulnerability Scans

- All LEAs will be enrolled in Dorkbot on July 1, 2023.
- Dorkbot is a free UT Austin service used to identify and verify vulnerabilities in web applications that have been targeted, using opensource reporting.
- When vulnerabilities are verified, LEA Cybersecurity Coordinators will be notified.
- LEAs that do not wish to participate can opt-out by emailing cybersecurity@tea.texas.gov.
- All verification scans will come from: autoscan.infosec.utexas.edu (146.6.15.11).
- Any reports associated with exploits and vulnerabilities can be exempted from PIR via the Attorney General's Office.



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>

The background of the slide is an aerial photograph of a city skyline, likely Austin, Texas, during the "golden hour" of late afternoon. The sky is a mix of light blue and orange, with scattered clouds. In the foreground, a river flows through the city, reflecting the sky and the buildings. The city is filled with various buildings, including a prominent tall skyscraper. The overall scene is vibrant and captures the essence of a modern urban environment.

Texas K12 Cybersecurity Program SentinelOne



Protecting Those Who Inspire Our Future Leaders

Jared Phipps- SVP Americas Sales & Solution Engineering
Jared.Phipps@SentinelOne.com

Brad R. Booth - Texas Public Sector
M) 214.578.5024
Brad.Booth@SentinelOne.com

¡Announcement!

**After today,
you should
know...**



Ransomware Roll-Back Remediation

Chromebook, iOS, Android, Legacy OS & More

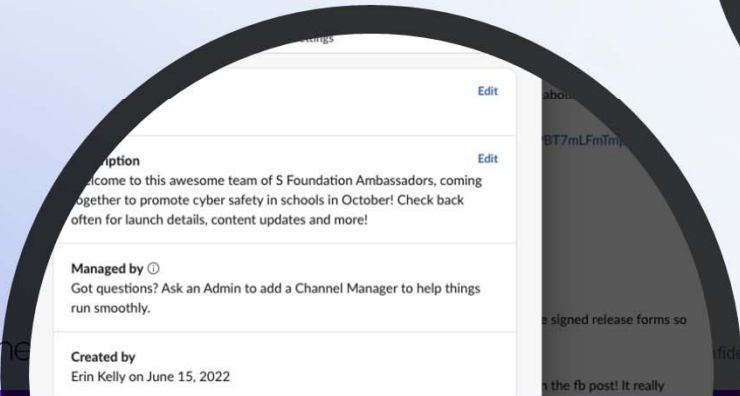
Block TikTok, XDR, DataLake, Intel, Future Proof

Together we can be a **Force For Good!**

S | Foundation

Securing a Safer Future for All

<https://www.sentinelone.com/s-foundation/>



SentinelOne's Future + Threat Trends & Demo



Jared Phipps

SVP, Americas Sales & Solution Engineering

San Antonio, TX

The Most Active Nation State Actors Year To Date

01

APT35

based in Iran 

02

Temp.Hex,

based in China 

03

APT30,

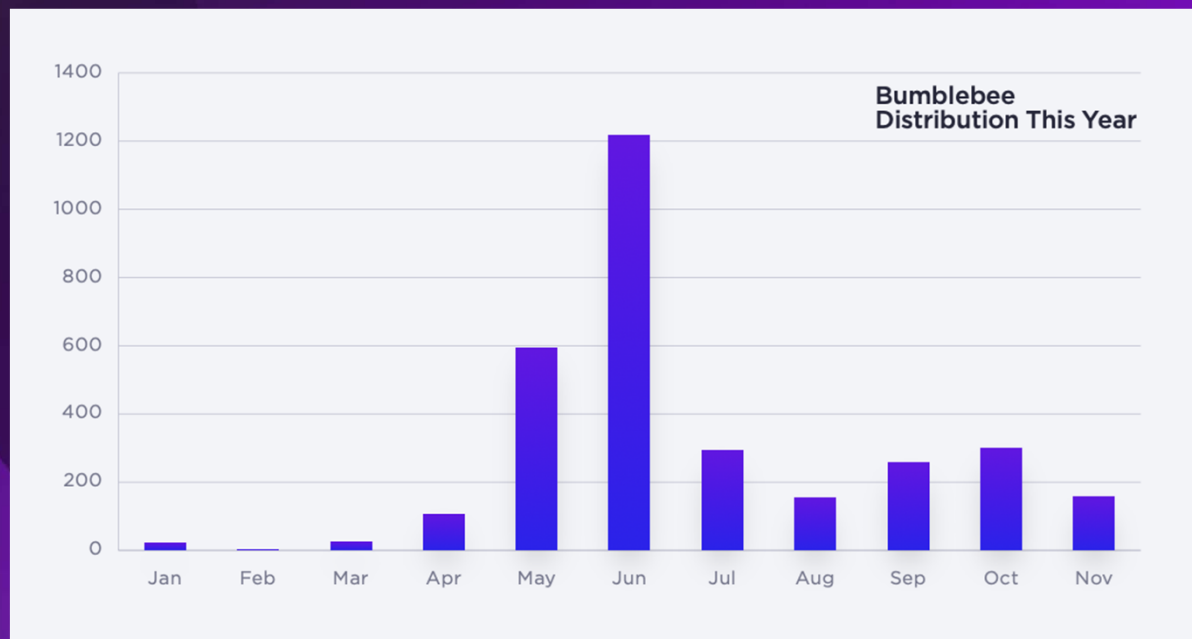
based in China 

04

Lazarus, based

in North Korea 

Ransomware Actors Resurging 2022 Year Completed



2022 Ransomware Groups Risk Matrix

Ransomware Group Names in bold are predicted to be highly active in 2023 as well.



Top Ransomware of 2023

1.Lockbit

1.AlpVM

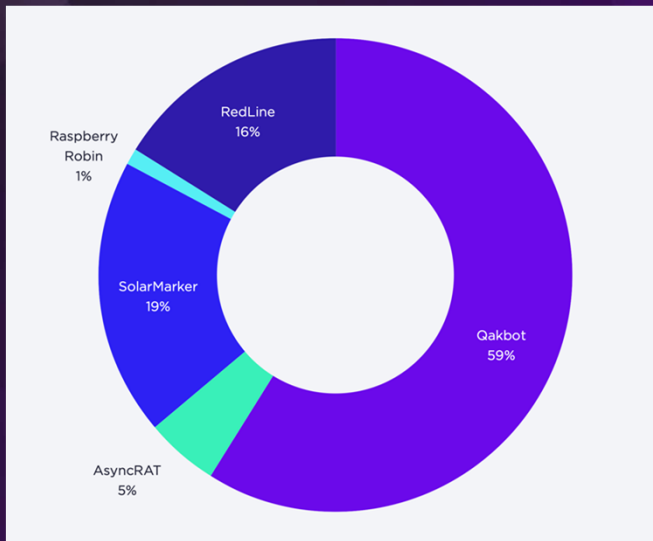
1.Vice Society

1.CLOP

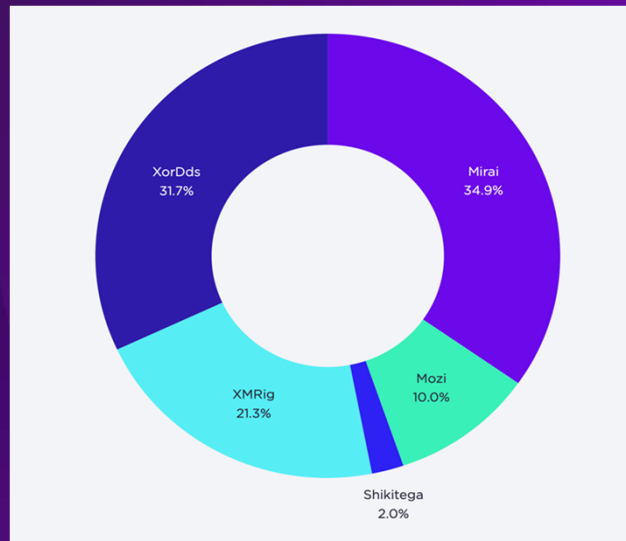
Lockbit has been the #1 ransomware worldwide 3 years running

Top Threats By OS

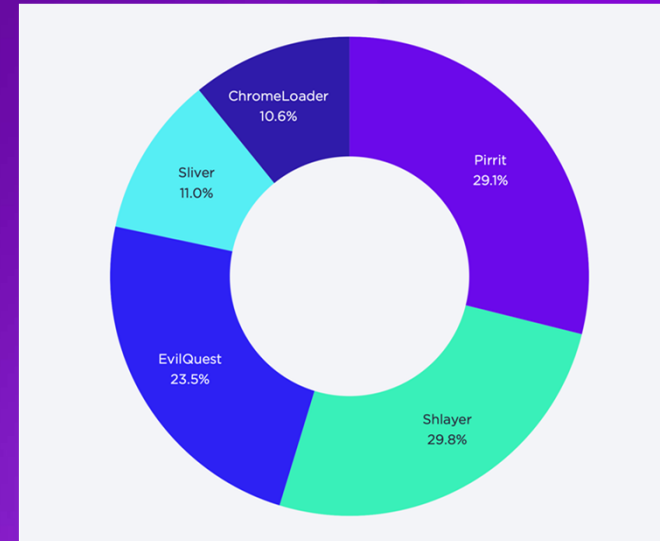
Windows



Linux



MacOS



Demo - Lockbit

TheBorg_RAD - VMware Workstation

File Edit View VM Tabs Help

TheBorg_RAD x

Manage Manage assimilation domain

File Home Share View Shortcut Tools Application Tools

scenarios > assimilation domain

| Name | Date modified | Type | Size |
|---------------------------------|----------------------|-------------------|--------|
| Adapt Payload.ps1 | 9/21/2022 1:12 PM | Windows PowerS... | 2 KB |
| Check Connectivity to Starships | 11/2/2022 10:53 PM | Shortcut | 2 KB |
| readme.txt | 11/10/2022 12:50 ... | Text Document | 1 KB |
| ResistancesFutile.exe | 9/22/2022 11:09 AM | Application | 960 KB |

4 items 1 item selected 1.22 KB

2:28 PM 4/20/2023

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

TheEnterprise_RAD - VMware Workstation

File Edit View VM Tabs Help

TheEnterprise_RAD x

Recycle Bin

kali file server

Sensitive - Shortcut

Sentinelinst... (1)

scenarios

Google Chrome

Windows 10 Enterprise
Windows License
Build 19041.vb_release.15

Type here to search

2:28 PM 4/20/2023

To direct input to this VM, click inside or press Ctrl+G.

TheMelbourne_Identity - VMware Workstation

File Edit View VM Tabs Help

TheMelbourne_Identity x

Recycle Bin

kali file server

Sensitive - Shortcut

Sentinelinst... (1)

scenarios

Endpoint-D...

Windows 10 Enterprise Evaluation
Windows License is expired
Build 19041.vb_release.19H2.1406

Type here to search

2:28 PM 4/20/2023

To direct input to this VM, click inside or press Ctrl+G.

TheSaratoga_Identity - VMware Workstation

File Edit View VM Tabs Help

TheSaratoga_Identity x

Recycle Bin

kali file server

Sensitive - Shortcut

Sentinelinst... (1)

scenarios

Google Chrome

Type here to search

4:28 PM 4/20/2023

To direct input to this VM, click inside or press Ctrl+G.


Type here to search

4:28 PM 4/20/2023

Earnings upcoming

4:28 PM 4/20/2023

NATIVE DATA

 EPP & EDR

 XDR

 Cloud

 Identity

 IR & MDR

Singularity™ Platform

Security DataLake

IDENTITY

EMAIL

CASB

SASE

WEB

THREAT INTEL

SANDBOX

FIREWALL

CASE MGMT

LOG INGEST

INGEST DATA FROM ANY SOURCE



The Value of

Singularity™ Platform

The Singularity Difference



Single Console & Platform

Consolidate vendors, train staff on ONE solution



Time to Value

Fully deploy and protect in days across entire enterprise



Lower TCO

Consolidate multiple agents and vendors. Data retention costs fraction of current usage



Unified Data Lake

Only security vendor built on a single unified data platform for security and operations



Open Ecosystem of Best-of-Breed Tools

Improve ROI of tools you already own



Unprecedented Protection

MITRE Leader with 100% Prevention



Superior Automation

Streamline SOC workflows



Ease of Use

Train staff on ONE solution only

Singularity™ Endpoint



Industry-Leading EPP/EDR

Fastest MTTR with highest accuracy. Free up resources to investigate what really matters



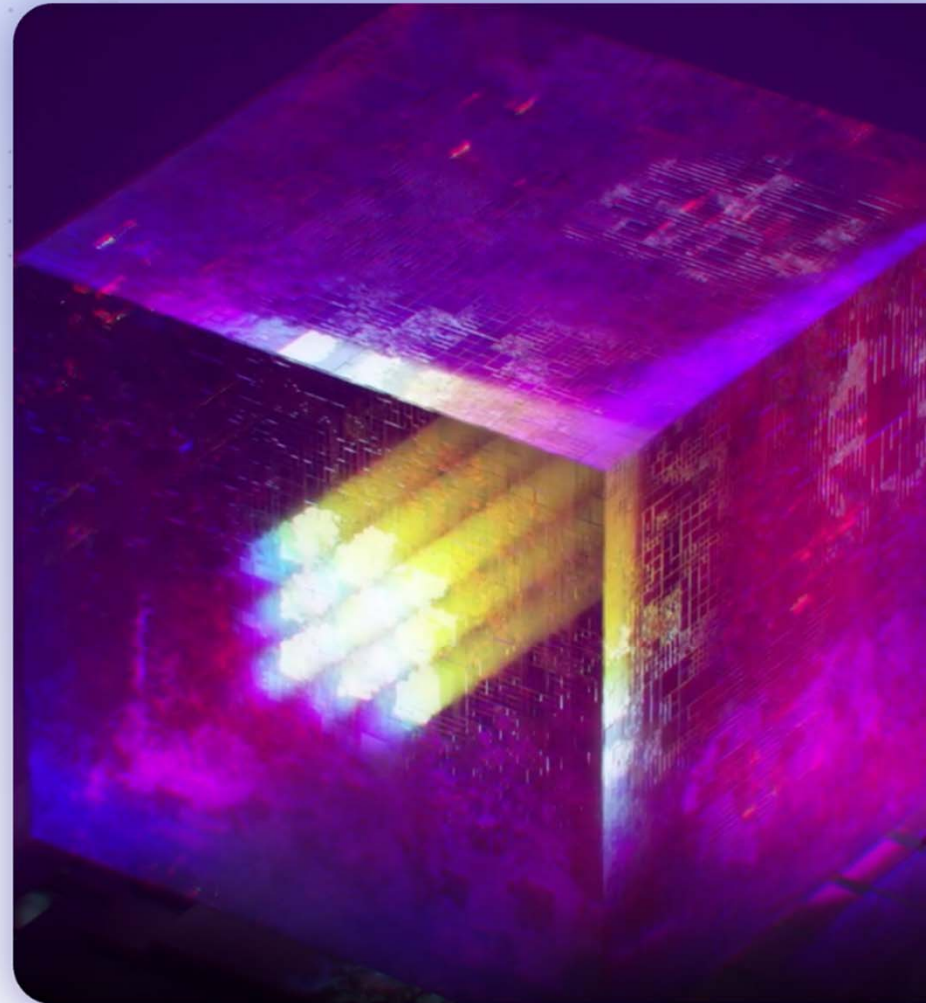
Streamlined Security

Single pane of glass. Improved security posture. Increased SOC efficiency driven by automation.




Increased Analyst Efficiency

Reduce alert fatigue and manual triage for SOC teams. ITSecOps tools provide additional value



Why SentinelOne?

Gartner

 Magic Quadrant

A Leader.

SentinelOne is a Leader in the 2023 Gartner Magic Quadrant for Endpoint Protection Platforms.

Gartner Ranks SentinelOne Highest Among All Vendors in Critical Capabilities


MITRE
ENGENUITY™

100% Protection Zero Misses

SentinelOne delivered full protection and was fastest to detect and block attacks.

Zero Delays

SentinelOne detections deliver on their promise out of the box, in real time, without delay.

Highest Analytic Coverage 3 Years Running

SentinelOne leads the pack in automatic correlation & contextualization of alerts.

Gartner
Peer Insights™

4.8 Rating



Across EPP, EDR, and CWPP

97% Would Recommend

Built Different = Better Results



100% Protection, Top Analytic Coverage, Zero Delays (2022 MITRE ATT&CK Evaluation)



Optimal for Prevention-Focused Orgs



1-Click Remediation & Rollback



Protection for ChromeOS, Legacy, iOS, Android & more



Want to onboard ahead of Sept 1?

Email us:

Brad.Booth@SentinelOne.com
Lindsay.Claussen@SentinelOne.com



sentinelone.com



SentinelOne®



Thank you!

Questions?

Email :

cybersecurity@tea.texas.gov