

Texas Education Agency (TEA) Managed Security Services (MSS) Webinar

Endpoint Detection and Response (EDR)

May 5, 2026



Agenda



- 1. Description of EDR services**
- 2. EDR Architecture By Service Offering**
- 3. Description of EDR services**
- 4. Benefits to you**
- 5. Engagement Process**
- 6. Questions and answers**



Managed Security Services- A New Way Of Doing Security For TEA



So What Is EDR Managed Services?

- A security operations function where the Managed Security Services (MSS) team operates, tunes, and responds through EDR tooling. Covering the entire lifecycle of endpoint detection.
 - CrowdStrike
 - SentinelOne

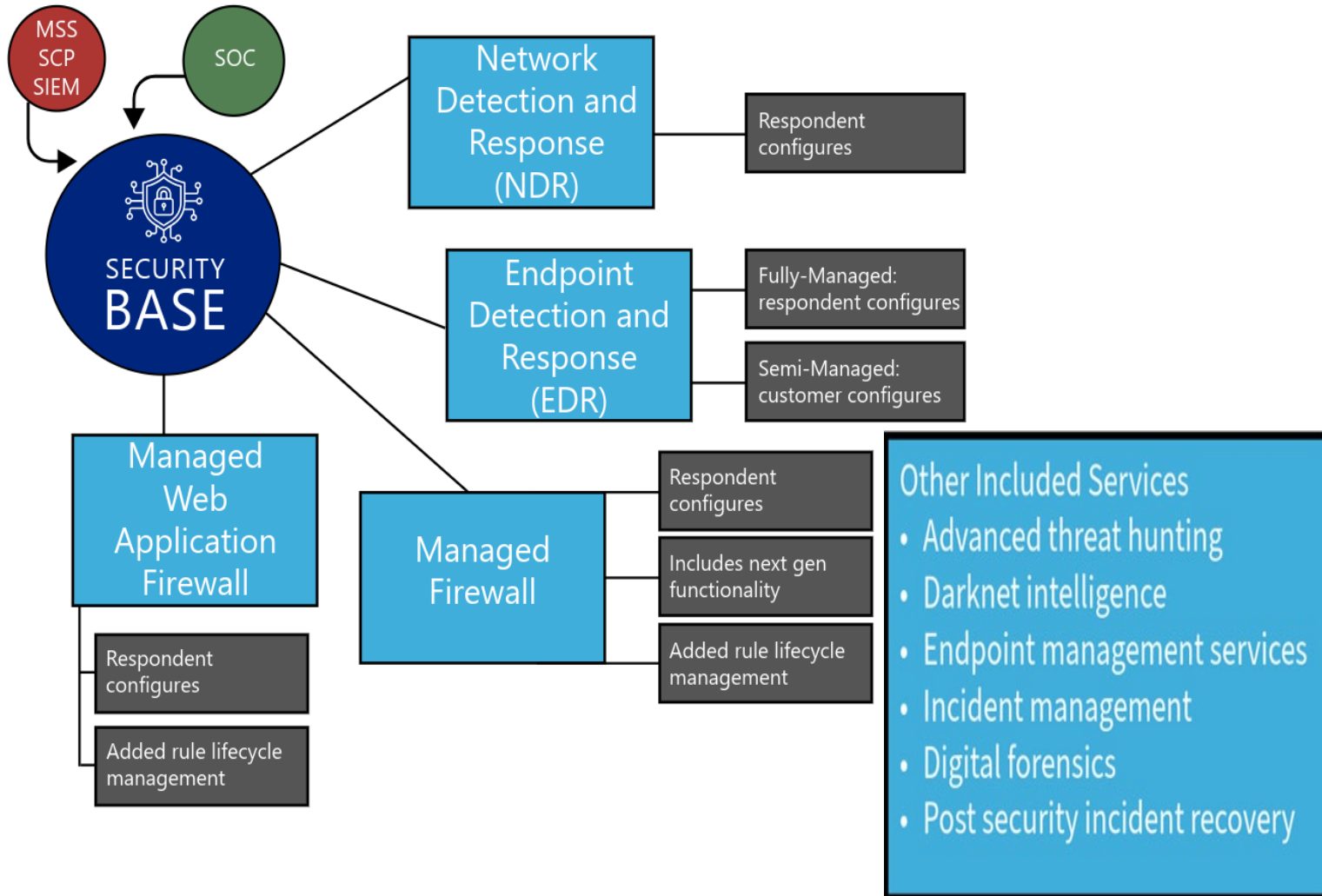
Why It Matters To You

- Offloads the high-volume, time-consuming operational work
- Dedicated and Shared ensures continuous monitoring 24/7 SOC
- Improves detection accuracy with dedicated analysts who know the tooling deeply

More Than Just You

- Managed Service reduces the staffing cost of SOC services for the entire state (it is more than just you)
- Faster incident containment for a more secure Texas
- Predictable cost per end point- the variable is the number of endpoints in your environment

MSS Service Overview



- Managed Security Services (MSS) is an offering within DIR's Shared Technology Services program providing a cost-effective solution to state, local, municipal, and higher-education cybersecurity needs
- MSS's goal is to provide strong and consistent management of state data security
- Integrated Platform for increasing overall security posture
- Service flexibility that supports Texas agencies that best fits their organization
- Full scope of services



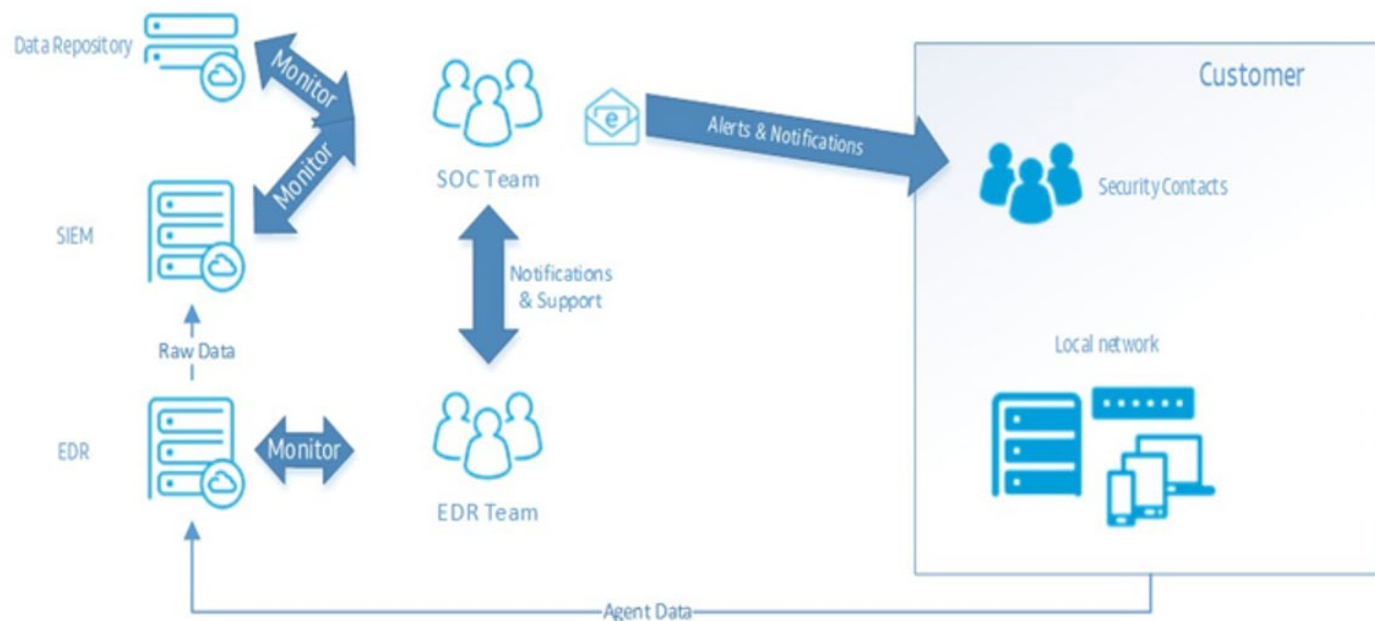
Benefits Of EDR Services: So Much More Than Just A License Cost

Direct Benefits To You:

1. **Enterprise-Grade EDR Platforms:** Best-in-class detection technology with advanced behavioral analytics and automated response workflows—deployed without capital expenditure
2. **24/7/365 Managed Operations:** Fully managed threat hunting, alert triage, and incident response eliminates need for specialized security staff and reduces operational overhead
3. **Reduced Mean Time to Detect/Respond (MTTD/MTTR):** Automated containment and expert SOC intervention minimize ransomware spread, system downtime, and recovery costs
4. **Regulatory Compliance Alignment:** Pre-configured controls meet CISA SCuBA, NIST 800-171, FERPA, and state cybersecurity mandates—with continuous compliance monitoring and audit-ready reporting
5. **Zero Learning Curve Deployment:** Turnkey managed service requires no specialized training or certifications for internal staff—Your team deploys the EDR Agent, SAIC handles detections, tuning, and ongoing management
6. **Strategic IT Resource Optimization:** Offloading security operations allows limited IT personnel to focus on educational/mission-critical initiatives rather than alert fatigue and threat analysis, managing a security console

Security Architecture - Shared EDR

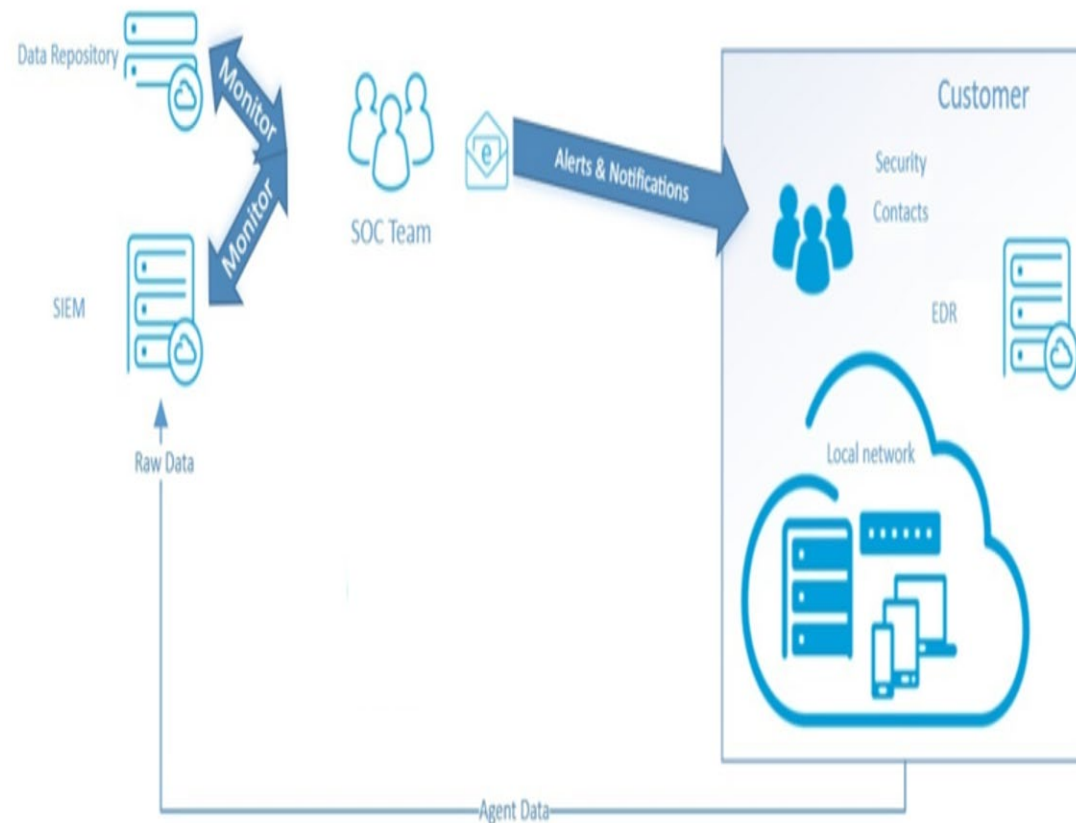
- **MSS EDR leverages vendor-provided tools and experienced security professionals** to monitor and manage endpoint protection across desktops, laptops, servers, and mobile devices.
- **Continuous monitoring is performed** for evidence of threats, indicators of compromise, and malware—providing response actions and/or alerts when an endpoint is potentially compromised.
- **The solution is delivered from a single, multi-tenant, cloud-based instance** of a supported EDR technology recommended as 'best-fit' by MSS and/or selected by the Customer.
- **EDR licensing, configuration, and management are included** as part of the MSS-managed service, reducing operational burden on the Customer.
- **MSS leverages existing security services** to provide greater insight on potential threats, impacts, and remediation responses for the Customer.



Platform Architecture

Security Architecture- Dedicated EDR

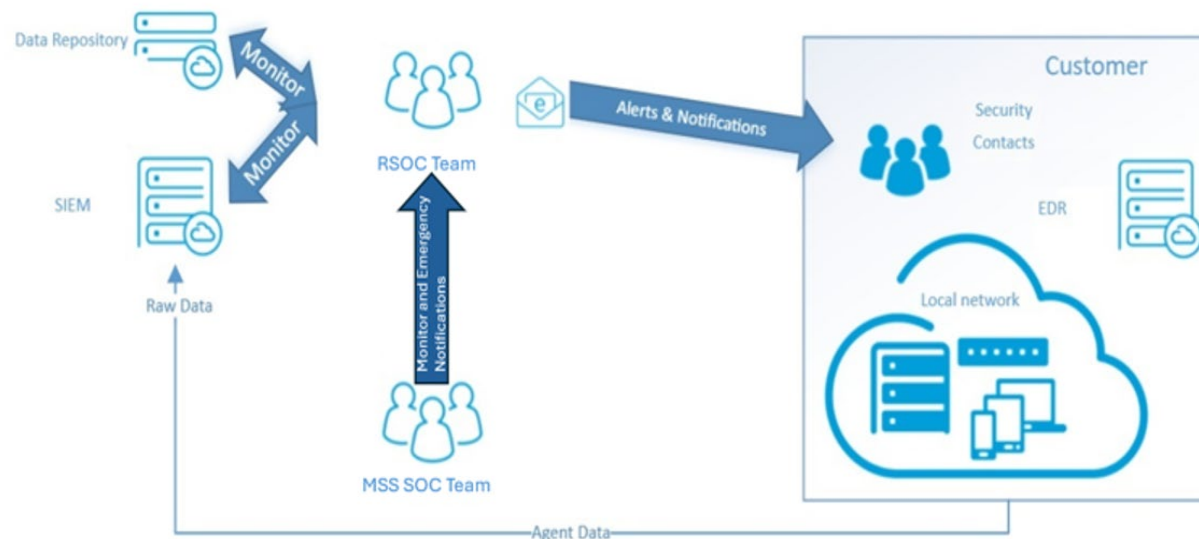
- **For entities retaining their existing CrowdStrike or SentinelOne solution**, MSS offers a Dedicated EDR Service that enhances monitoring and alerting by leveraging additional data and context from other MSS Services.
- **The Customer maintains full ownership** of their current EDR solution, including licensing, vendor support, management, monitoring, and response activities.
- **The Customer forwards EDR events** (via API/Syslog) to MSS for ingestion into the MSS Shared Services SIEM.
- **MSS cross-correlates EDR events** against state-wide data from other MSS services, delivering alerts and notifications on detected threats, indicators of compromise, and/or malware.



Platform Architecture

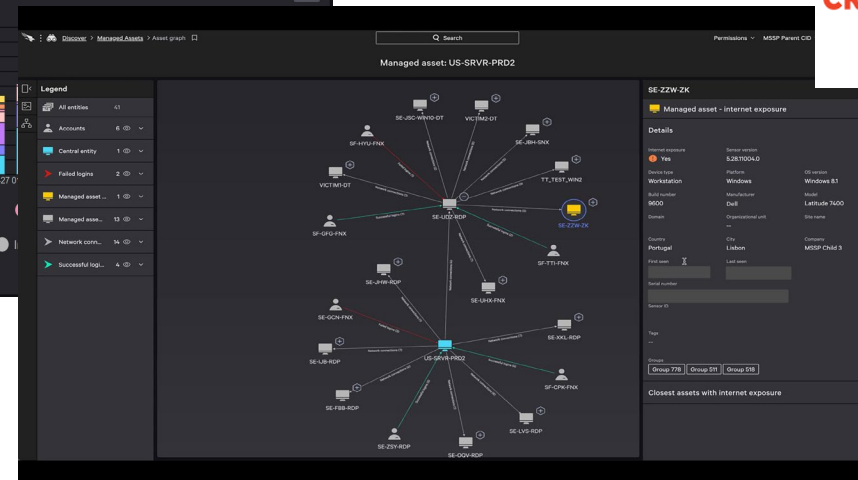
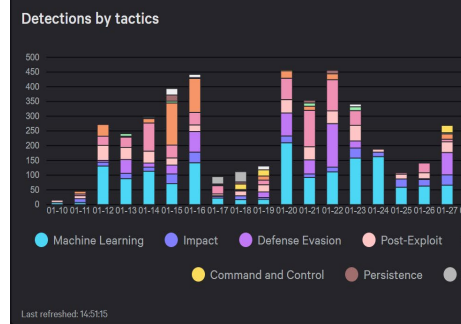
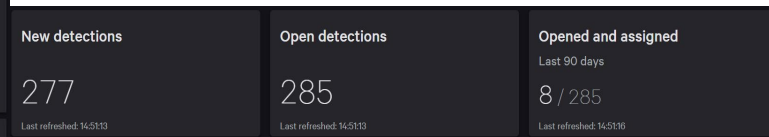
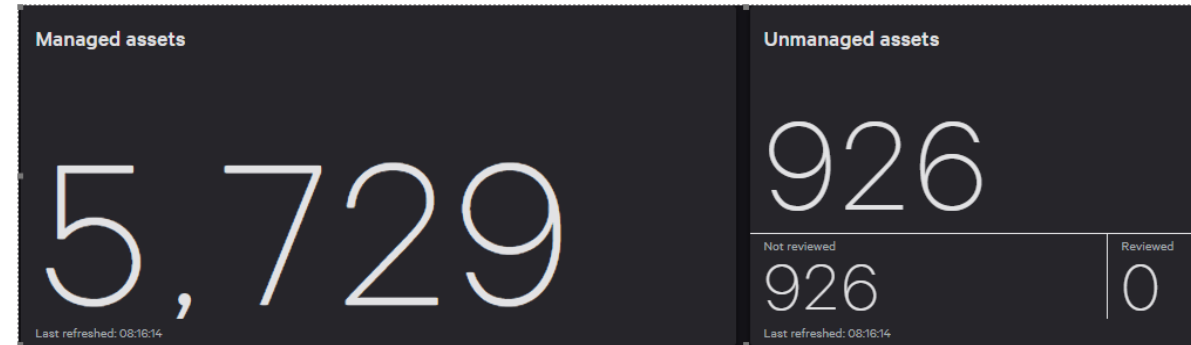
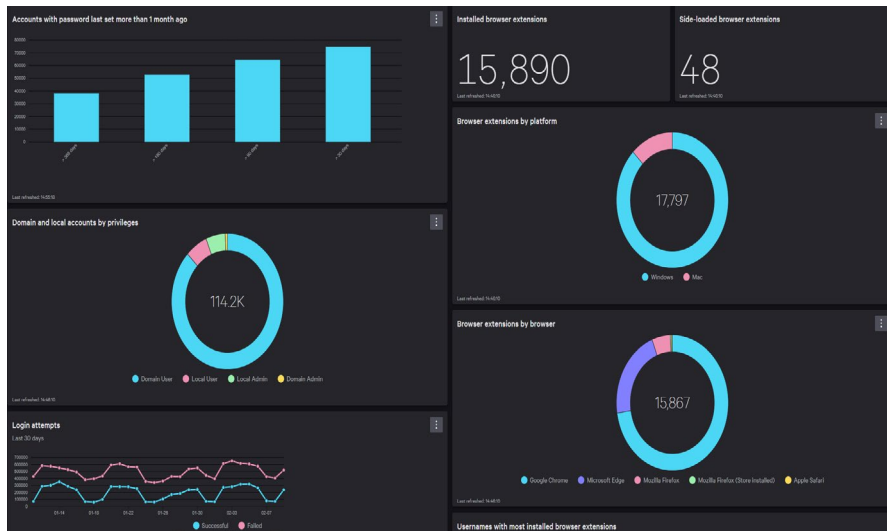
Security Architecture- Dedicated RSOC

- **MSS establishes a multi-tenant, dedicated EDR instance** for the sole use of the DIR Customer-designated RSOC, who maintains EDR configuration for all of their respective customers.
- **Comprehensive licenses and detailed installation instructions** are provided to enable the managing RSOC to efficiently deploy EDR software on intended devices or support their customers with installation actions.
- **The RSOC EDR console integrates with the MSS SCP SIEM**, enabling the MSS SOC to ingest event data and provide monitoring, alerting, triage, analysis, and response in support of RSOC operations.
- **Automated notifications are delivered to the RSOC** for detected events, malicious activities, and potential data breaches; if no RSOC action is observed, MSS escalates with incident response information.
- **Event data is maintained and accessible via a read-only web portal** through the STS Portal—including activity dates, device identities, EDR engines used, detected activity descriptions, and mitigation actions taken.



Platform Architecture

Your Endpoints Have Much To Say- More Than A Slide Can Hold...



Our Best-in-Class tools help you listen

"Deep Visibility" Into Your Security Events

Threat Status: NOT MITIGATED | AI Confidence Level: **SUSPICIOUS** | Analyst Verdict: Undefined

No actions taken yet

NETWORK HISTORY

First seen Nov 29, 2022 13:19:31
Last seen Nov 27, 2023 13:41:53

102 times on 76 endpoints
3 Accounts / 29 Sites / 35 Groups

THREAT FILE NAME python3.7

Path /host/run/containerd/io.containerd.runtime.v2.task/k8s.io/7d9665731e14...

```

| filter(event.type == "IP Connect" AND event.network.direction == "OUTGOING" AND src.process.displayName == "Windows PowerShell" AND !net_private(dst.ip.address) AND !net_ipsubnet(
dst.ip.address, "0.0.0.0/8") AND !net_ipsubnet(dst.ip.address, "127.0.0.0/8") AND !net_ipsubnet(dst.ip.address, "169.254.0.0/16"))
| columns event.time, event.id, event.type, site.id, site.name, agent.uuid, src.process.storyline.id, src.process.user, src.process.uid, src.process.cmdline, src.process.image.path, dst.ip.address,
dst.port.number, event.network.direction, event.network.protocolName, event.network.connectionStatus
| sort - event.time
| limit 1000
                    
```

All Events 345 | Indicators 345

Processes

Search Processes...

Process	Pid	Date
News	12737	Jan 24, 2020 18:21
parentalcontrols	12735	Jan 24, 2020 18:21
parentalcontrols	12731	Jan 24, 2020 18:21
syncdefaults	12728	Jan 24, 2020 18:21
parentalcontrols	12726	Jan 24, 2020 18:21
parentalcontrols	12720	Jan 24, 2020 18:21
parentalcontrols	12716	Jan 24, 2020 18:20

launchd Events: 38897

- parentalcontrols Single Node
- parentalcontrols Single Node
- com.apple.iCloudH... Single Node
- parentalcontrols Single Node
- News Single Node
- parentalcontrols Single Node

556 results found from Nov 16, 2024 19:28:47 to Nov 17, 2024 19:28:47

Table

Source Process Unique ID	Source Process Command Line
powershell.exe 8BF23F49D9E55BF0	C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy AllSigned -NoProfile -NonIn
powershell.exe 69F549B205E7700	C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy AllSigned -NoProfile -NonIn
powershell.exe F6EE6CB35AC64C10	"Powershell.exe" -ExecutionPolicy Unrestricted -WindowStyle Hidden -File "C:\Packages\Plugins\Microsof
powershell.exe DFED6CB35AC64C10	"Powershell.exe" -ExecutionPolicy Unrestricted -WindowStyle Hidden -File "C:\Packages\Plugins\Microsof
powershell.exe C098FEE34D32253	C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy AllSigned -NoProfile -NonIn
powershell.exe 031B250A848FF6A	C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy AllSigned -NoProfile -NonIn

Threat Status: NOT MITIGATED | AI Confidence Level: SUSPICIOUS | Analyst Verdict: Undefined | Incident Status: Unresolved

Identified Time Nov 27, 2023 13:41:53
Reporting Time Nov 27, 2023 13:41:53

No actions taken yet

Processes

central-1.compute.internal

Search Process

Process	Pid	Date
containerd-shim...	27373	Nov 27, 2023 13:31:54
bash	27594	Nov 27, 2023 13:31:55
apache2	28001	Nov 27, 2023 13:31:57
apache2	28009	Nov 27, 2023 13:31:57
dash	33661	Nov 27, 2023 13:41:38
bash	33705	Nov 27, 2023 13:41:41
python3.7	33823	Nov 27, 2023 13:41:52

```

graph LR
    A[containerd-shim... One Child] --> B[bash One Child]
    B --> C[apache2 One Child]
    C --> D[apache2 One Child]
                    
```

EVENTS COUNTS

2 All Events | 2 Processes

PROCESS SUMMARY

Name: bash
UID: 9b51436d-ec79-0787-ac3c-51ba04936276, 27594
ID: 27594
Command Line: /bin/bash /main.sh
Image Path: /bin/bash
SHA1: f9d351e05d6bed9776d404c17ab77752e774e9
Root: False
Verified Status: N/A
Has Active Content: N/A

Both In Real Time And With Historical Data

Things To Know To Set Expectations



New Customers

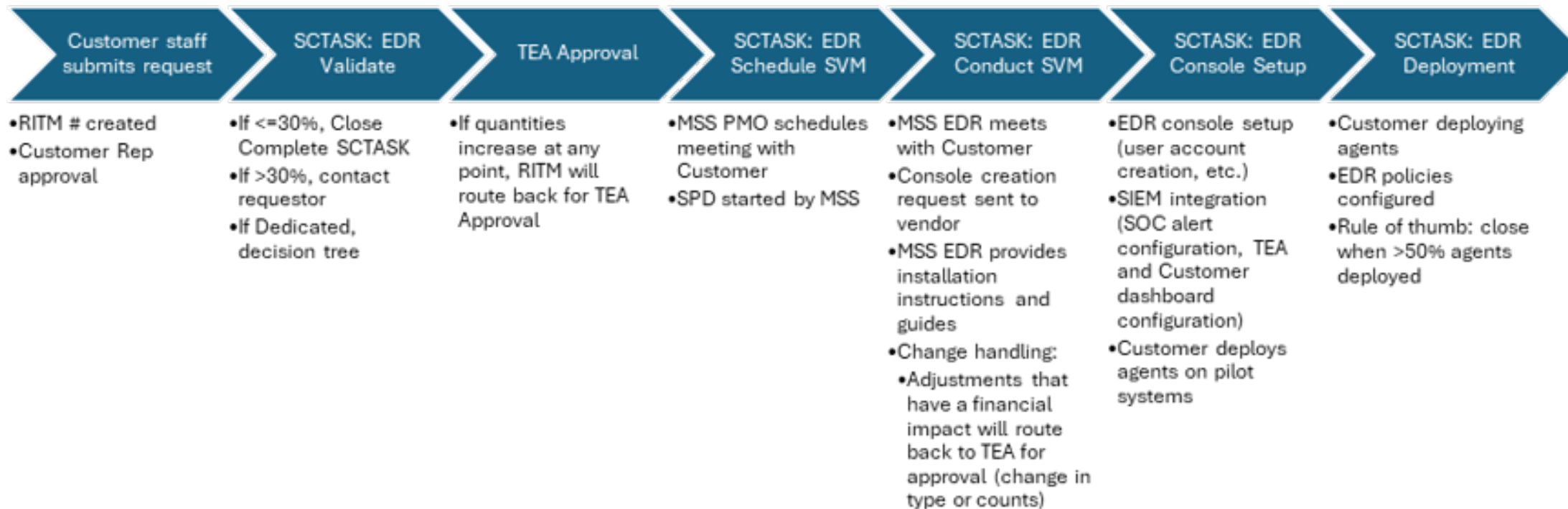
- TEA will limit the distribution to school systems with a total enrollment of 50,000 and below
- A range from 30 licenses up to licenses equal to 30% of student enrollment, whichever is larger
- Start with the Portal- [DIR STS Portal](#)
 - Outlines service description and service options for EDR
 - This is "how" you begin the process- Creates the **RITM**
- Engaging with the MSS
 - Once approved the MSS will reach out and schedule a Kick-Off

Existing Customers

- We encourage you to make full use of your total approved EDR licenses
 - Unused license means someone else does not have access to EDR
 - If you need more- Use the Add-On Process and include your justification
 - School systems have 60 days to deploy to 90% of requested agents
- Engaging with the MSS
 - The MSS has folks who can assist you in getting the most out of your EDR service:
[L TXDIR MSS Outreach@saic.com](mailto:L_TXDIR_MSS_Outreach@saic.com)
 - [L TXDIR MSS EDR@saic.com](mailto:L_TXDIR_MSS_EDR@saic.com)

EDR Workflow For New TEA Provided Services

IT all starts with a ticket through the portal- [DIR STS Portal](#)






You Are Part Of The Process- Your Approvals

Note: after you submit a ticket, you must also then approve!

<https://txdir.servicenowservices.com/sp?id=approvals>

Home > Approvals Search the Service Portal 🔍

 **Approval Central Dashboard**
Click here to view outstanding and past approvals across a variety of reports.

☰ My Approvals

Number	Group or Approver	Short Description	State	Created On	Due Date
RITM1240572	TEA EDR Approval	\$ EDR (Endpoint Detection and Response) - SAIC - ISD - Region 3 - Yoakum ISD EDR	Requested	2026-04-29 15:32:39	2026-04-29 15:32:39
RITM1240610	TEA EDR Approval	\$ EDR (Endpoint Detection and Response) - SAIC - CS - Jubilee Academies EDR	Requested	2026-04-29 15:32:35	2026-04-29 15:32:35
RITM1240612	TEA EDR Approval	\$ EDR (Endpoint Detection and Response) - SAIC - ISD - Region 3 - Bloomington ISD EDR	Requested	2026-04-29 15:32:31	2026-04-29 15:32:31
RITM1241462	TEA EDR Approval	\$ EDR (Endpoint Detection and Response) - SAIC - ISD - Region 20 - Uvalde CISD EDR	Requested	2026-04-29 15:32:27	2026-04-29 15:32:27
RITM1241611	TEA EDR Approval	\$ EDR (Endpoint Detection and Response) - SAIC - ISD - Region 1 - La Joya ISD EDR	Requested	2026-04-29 15:32:19	2026-04-29 15:32:19
RITM1241612	TEA EDR Approval	\$ EDR (Endpoint Detection and Response) - SAIC - ISD - Region 20 - South San Antonio EDR	Requested	2026-04-29 15:32:15	2026-04-29 15:32:15

Need More Help?- It Starts With The Portal



MSS Access Request

Submit a MSS Access Request



Please use this catalog item if you have an employee that needs to request new access to our MSS Services. These services include:

- SOC Services (SIEM Dashboard)
- EDR Console
- NDR Console
- Vuln Scanning Console (Recurring) Management
- Endpoint Management Console
- Managed Firewall
- WAF

Please answer the questions below. Questions with an asterisk are required.

* Indicates required

* Requested For

Requested By

* Provide brief 40 character summary

* Are you the Primary Contact for this request?

- Need assistance to access your console
- Console login issues or credentials
- Change who has access to the console

https://txdir.servicenowservices.com/sp?id=sc_cat_item&sys_id=6324e7d51bfba2d0c462cbf5624bcb71&sysparm_category=9955beb91bfed054a04b74c8dc4bcbd7

MSS Other Operational Services - SAIC

Submit a MSS Other Operational Services Request



Please use this catalog item to requests to MSS Services and Support that are not tied to other catalog items. These tasks include things such as access to SaaS platforms (CrowdStrike, SentinelOne, etc.), Access to the MSS Azure/Sentinel environment, or simply just to ask a question of our team. We're more than happy to assist with mostly any request that doesn't fit into one of the standard forms.

If you have any specific asks for MSS, please view the Managed Security Services requests located [here](#).

Please answer the questions below. All questions with an asterisk are required.

* Indicates required

* Requested For

Requested By

* Provide brief 40 character summary

* Are you the Primary Contact for this request?

- Experiencing Technical Issues
- Need to tweak your EDR settings
- Update your SOC alerts or contact list
- EDR Configurations

https://txdir.servicenowservices.com/sp?id=sc_cat_item&sys_id=b903fd2087f83290f49ca9760cbb35ae&sysparm_category=9955beb91bfed054a04b74c8dc4bcbd7

Stay Informed And Primary Points of Contact



Stay Informed and Up To Date

- [TEA Cybersecurity Initiative Website:](https://tea.texas.gov/academics/learning-support-and-programs/technology-planning/k-12-cybersecurity-initiative)
<https://tea.texas.gov/academics/learning-support-and-programs/technology-planning/k-12-cybersecurity-initiative>
 - Steps for onboarding school systems to DIR Shared Technology Services (STS) portal
 - Updates about the program
 - Frequently asked questions about the program
 - Handy link to sign up for the Cybersecurity Coordinator Forum meetings
 - Previous K-12 Cybersecurity Initiative Webinars posted on this page
- TEA Program Email: k12cyber@tea.texas.gov

For More Information about Manage Security Services

Endpoint Detection and Response Team:

L_TXDIR_MSS_EDR@saic.com

Service requests:

<https://dir.texas.gov/it-solutions-and-services>

General engagement:

MSI Service Desk: +1 877-767-0656

L_TXDIR_MSS_Outreach@saic.com



About DIR Shared Technology Services (STS)

DIR's Shared Technology Services program provides government and higher education organizations with access to managed IT as a service, allowing customers to focus resources on supporting their mission and business functions rather than directly managing IT services.