LONI SOC-as-a-Service Offering

2024 Louisiana Higher Education Fiscal Summit

November 6th

Pennington Biomedical Research Center

Craig Woolley – LSU

Lonnie Leger – LONI

Cyber security attack headlines

Louisiana colleges restoring systems after state police find 'indicators of compromise'

Jonathan Greig | The Record from Recorded Future News
March 27th, 2023

Apparent cyberattacks hit 7 Louisiana colleges in 4 months: 'I'm hoping it's a wake up call.'

University of New Orleans among schools most recently reporting computer system disruptions

By MARIE FAZIO | Staff writer and LARA NICHOLSON | Staff writer   Mar 27, 2023

The OMV data breach is latest in string of Louisiana attacks; here are the others

By SAUL PINK | Staff writer   Jun 16, 2023   📖 1 min to read

Cyber attack causes college to cancel classes

January 21, 2024 / Gabriel Lucich / 2 Comments

Cyber News Rundown: Two more U.S. universities fall victim to ransomware

Posted by Tamara for OpenText on Mar 13th, 2023 at 11:16 AM

Kansas State University cyberattack disrupts IT network and services
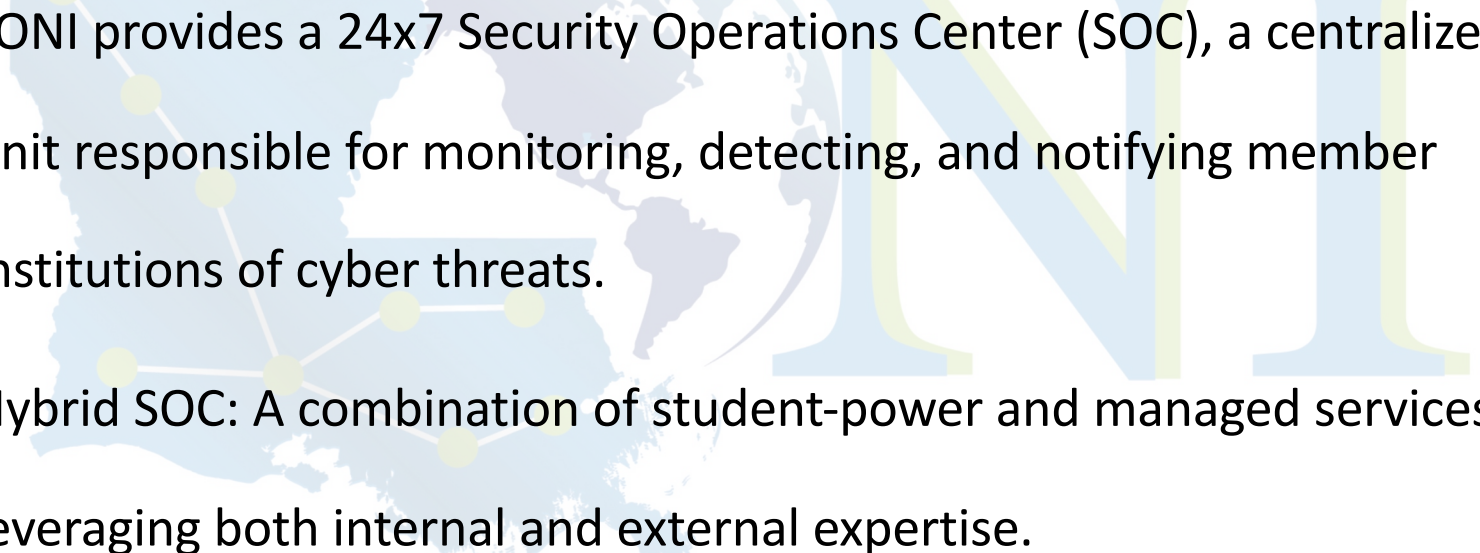
By Bill Toulas
📅 January 18, 2024   ⏰ 01:44 PM   💬 0

Mississippi Health System Ransomware Attack Affects 253,000

Report to State Regulators Indicates Big Jump in Number of Patients Affected

Marianne Kolbasuk McGee (🐦HealthInfoSec) • January 15, 2024   💬

What is the LONI SOC?

- LONI provides a 24x7 Security Operations Center (SOC), a centralized unit responsible for monitoring, detecting, and notifying member institutions of cyber threats.

- Hybrid SOC: A combination of student-power and managed services leveraging both internal and external expertise.

SOC project goals

- Increase the cyber security posture of Higher Education in the State of Louisiana

- Give Louisiana students great real world SOC experience

- Keep costs down

- Leverage Louisiana Optical Network Infrastructure (LONI)

- Increase collaboration across the state

- Find a Managed Detection and Response (MDR) provider to partner with
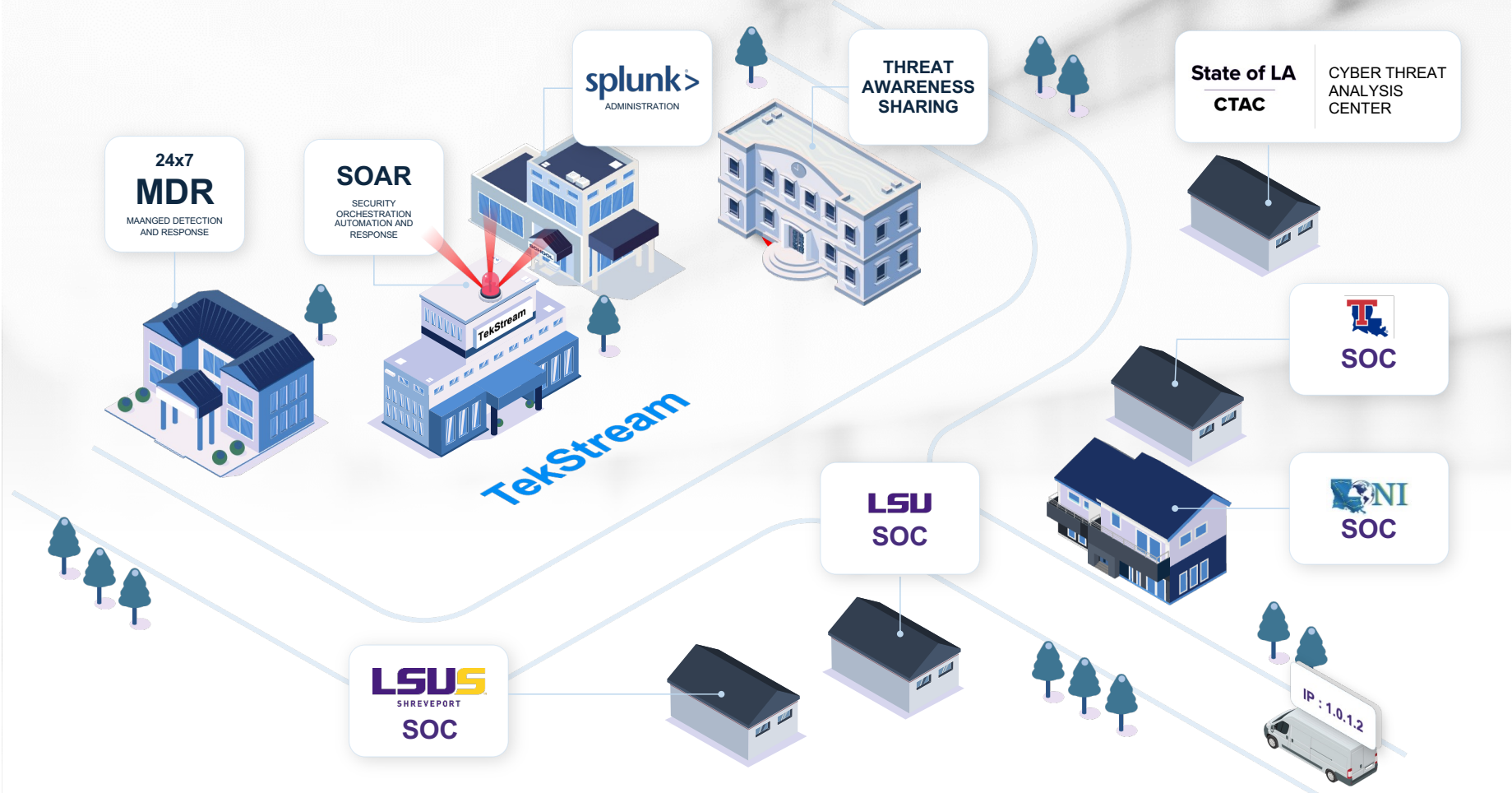
SOC ribbon cutting

[Video](#)

LONI student security analyst training/ onboarding process

1

2 **Training**
- Basic IT
- Splunk Training
- Runbook Training

3

4 **SOC Onboarding**

5 **MDR Training**

6

7

Initial Onboarding
- Critical Thinking Assessment
- Basic IT Assessment
- Interviews

Evaluation

- Cybersecurity Assessment
- Tool Assessment

- 1-2 Weeks Shadowing
- 1-2 Weeks Reverse Shadowing

- SA Maturity Levelling for Complexity and Career Planning
- On-going training (technical concepts, cybersecurity concepts)

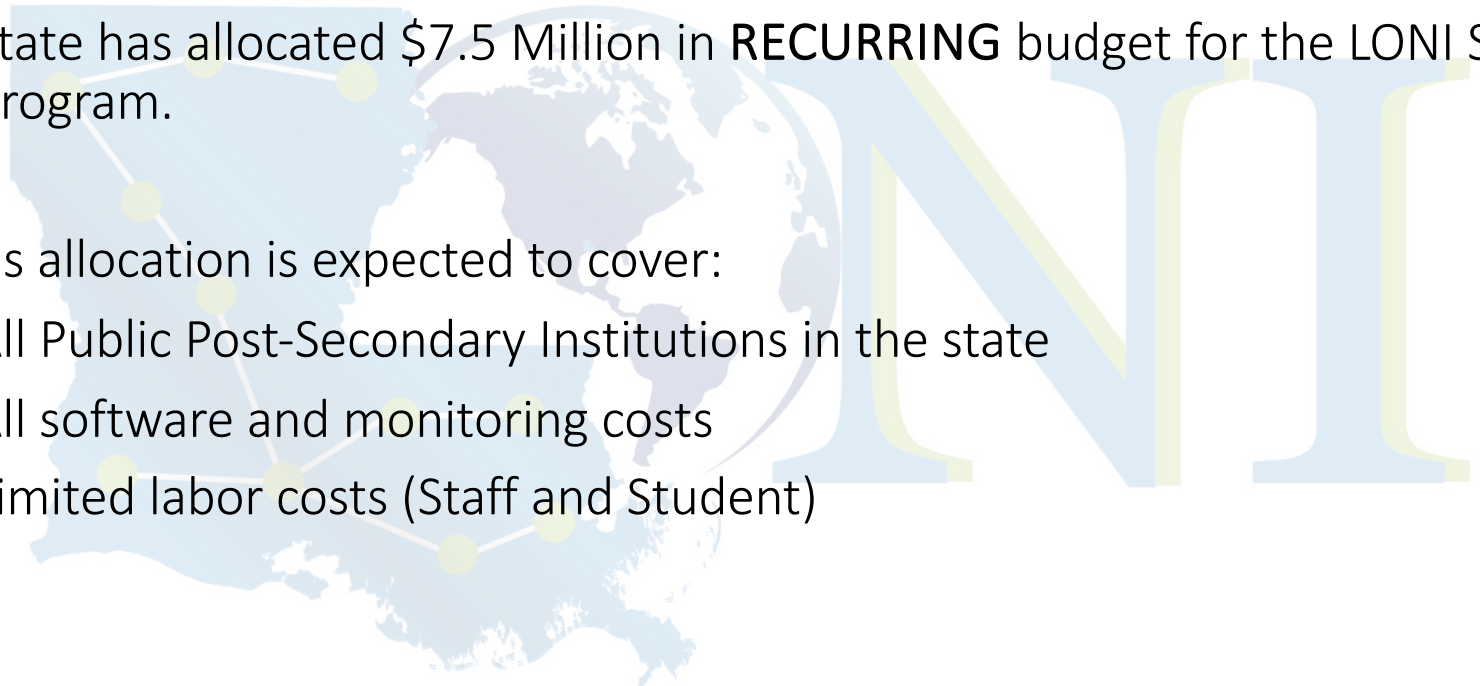- Placement (TS, state, federal, commercial

← 6 WEEKS →

← ONGOING →

Budget Allocation

- State has allocated $7.5 Million in **RECURRING** budget for the LONI SOC program.

This allocation is expected to cover:

- All Public Post-Secondary Institutions in the state

- All software and monitoring costs

- Limited labor costs (Staff and Student)

Rural Health Care Program

- LONI has worked with the University of Arkansas Medical System (UAMS) to encourage LONI member institutions to join the UAMS e-Link consortium.

- UAMS e-Link assists its qualified consortium members in applying to receive RHC funding for eligible services from LONI.

- If awarded, the member institution could receive a rebate up to 65% of their total LONI costs.

RHC Service Funding Case Study Comparing Total Benefit with & w/o SOC

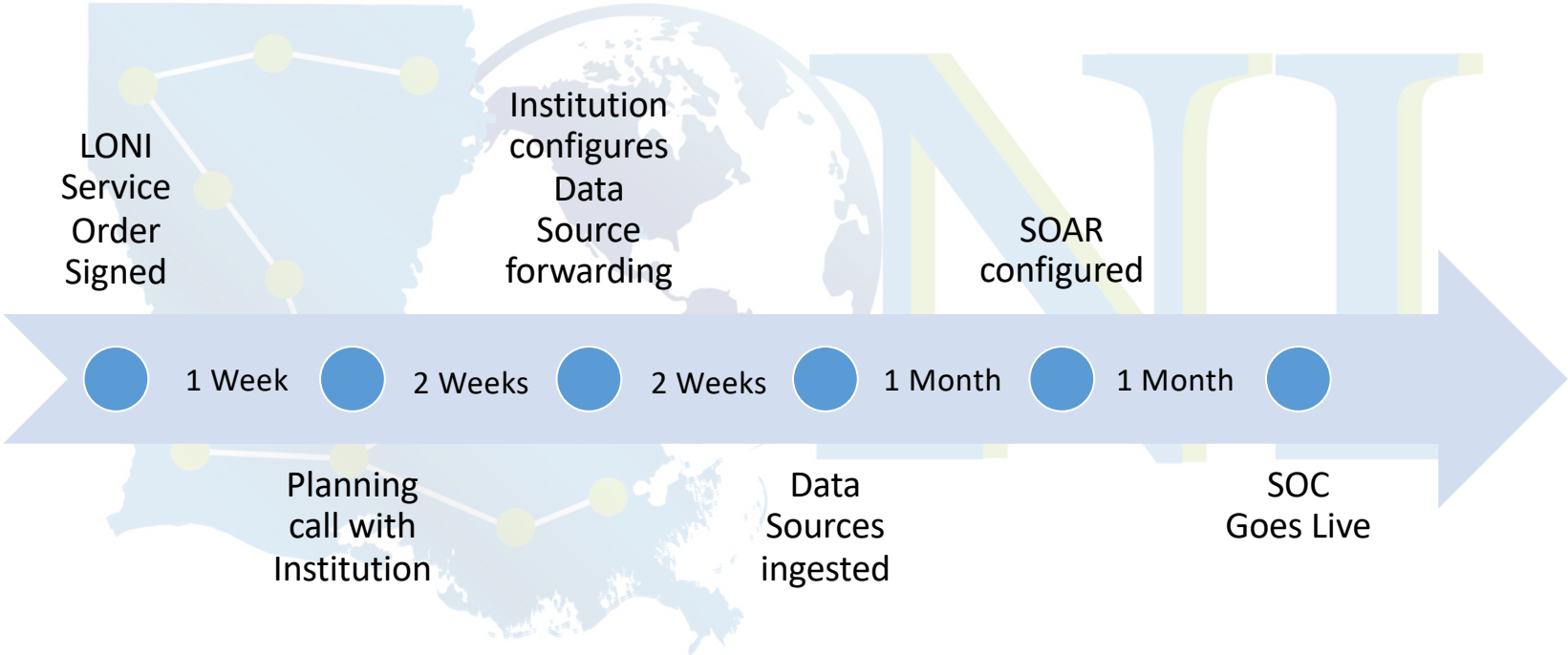| LONI Membership Fee	Small	Medium	Large
Total LONI Services	$60,000	$80,000	$100,000
RHC/UAMS w/o SOC (Reimbursement)	**$39,000**	**$52,000**	**$65,000**
LONI SOC Fee (BOR Funding)*	$193,000	$232,000	$451,000
Total LONI Services	$253,000	$312,000	$551,000
RHC/UAMS w/ SOC (Reimbursement)	**$164,450**	**$202,800**	**$358,150**

*BOR will transfer funds to each institution per their LONI Service Order for their allocated costs.
 Member institution will pay LONI thereby enabling Rural Health Care eligibility.

Current LONI SOC Customers

ULS	SUS	LSU	LCTCS
LaTech	SUBR	LSU	LCTCS
Northwestern	SULC	LSUHSC-NO	RPCC
Nicholls		LSUS	LDCC
ULL		LSUE	NLTCC
ULM*		LSUHSC-S	CLTCC
		LSUA	SOWELA*
		LSU Ag*	
		PBRC*	

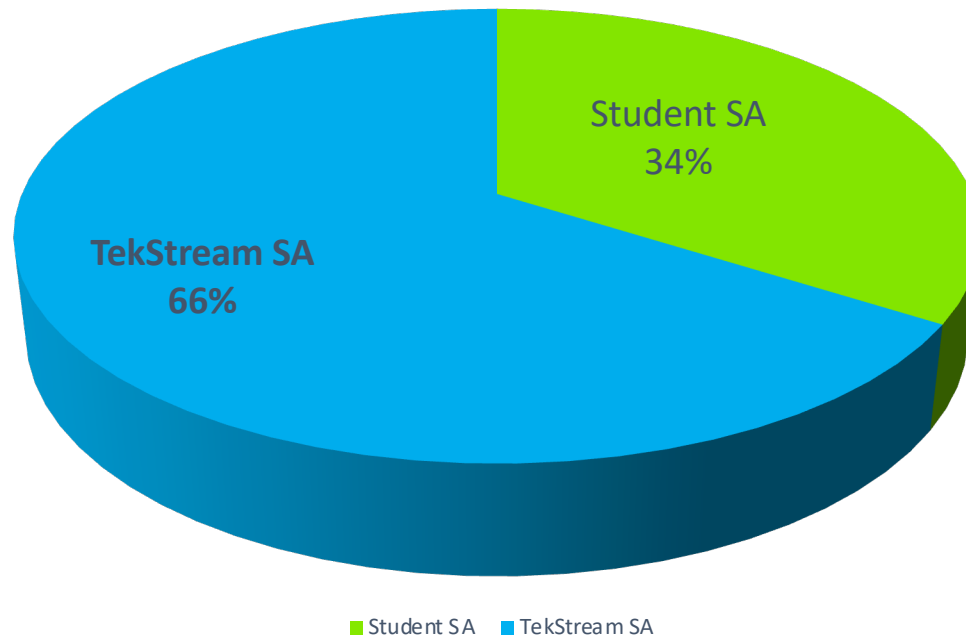* Scheduled "Go-Live" by Dec 31, 2024

Service Implementation

Total SOC Incidents 7/1/24 – 9/30/24

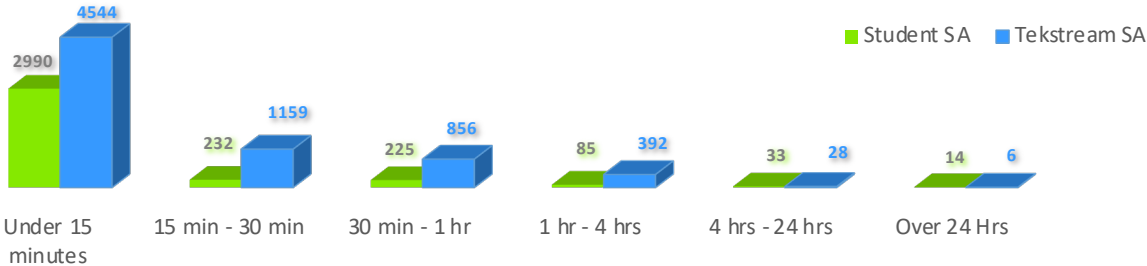- Total incidents: 10564
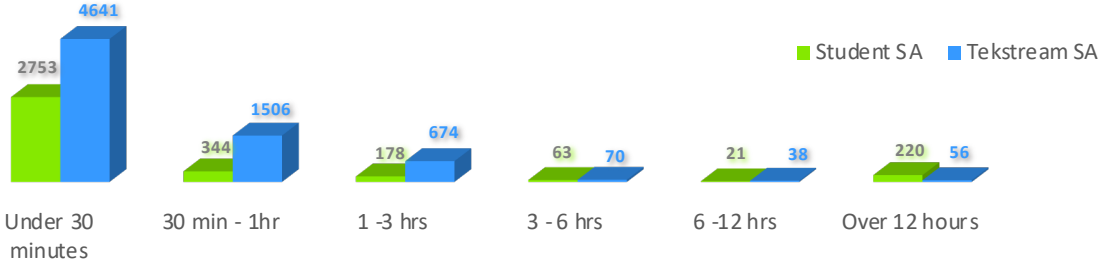- Total true positives: 654

Total Owned Incidents 7/1/24 – 9/30/24

Student SA 34%

TekStream SA 66%

■ Student SA ■ TekStream SA

Incident Metrics 7/1/24 – 9/30/24

Time to Assignment

Legend: Student SA, Tekstream SA

Category	Student SA	Tekstream SA
Under 15 minutes	2990	4544
15 min - 30 min	232	1159
30 min - 1 hr	225	856
1 hr - 4 hrs	85	392
4 hrs - 24 hrs	33	28
Over 24 Hrs	14	6

Time to Resolution

Legend: Student SA, Tekstream SA

Category	Student SA	Tekstream SA
Under 30 minutes	2753	4641
30 min - 1hr	344	1506
1 -3 hrs	178	674
3 - 6 hrs	63	70
6 -12 hrs	21	38
Over 12 hours	220	56

Questions?

Contact Us

"Thank you for your partnership with LONI."

www.loni.org

Follow us on Twitter: @LONI_LSU

Follow us on LinkedIn: Louisiana Optical Network Infrastructure