SECURITY OPERATIONS CENTER

Lance Neal, Executive Director, LONI
Craig Woolley, CIO, LSU

Why is this important?

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

Michigan community colleges recovering from cyber attacks

By Capital News Service | March 21, 2025

An Apparent Mass Hack at Penn Exposes Higher Ed's Security Weaknesses

By Ellie Davis | November 4, 2025

Cyber attack causes college to cancel classes

January 21, 2024 / Gabriel Lucich / 2 Comments

180 ransomware attacks plague education sector worldwide in 2025 through Q3

Published Oct. 30, 2025

August 12, 2025

Hack at Columbia Hits 870K People

Ransomware attacks in education jump 23% year over year

The first six months in 2025 saw 130 confirmed and unconfirmed ransomware attacks against colleges and schools, according to a report from Comparitech.

Published July 25, 2025

Anthropic Says Chinese Hackers Used Its A.I. in Online Attack

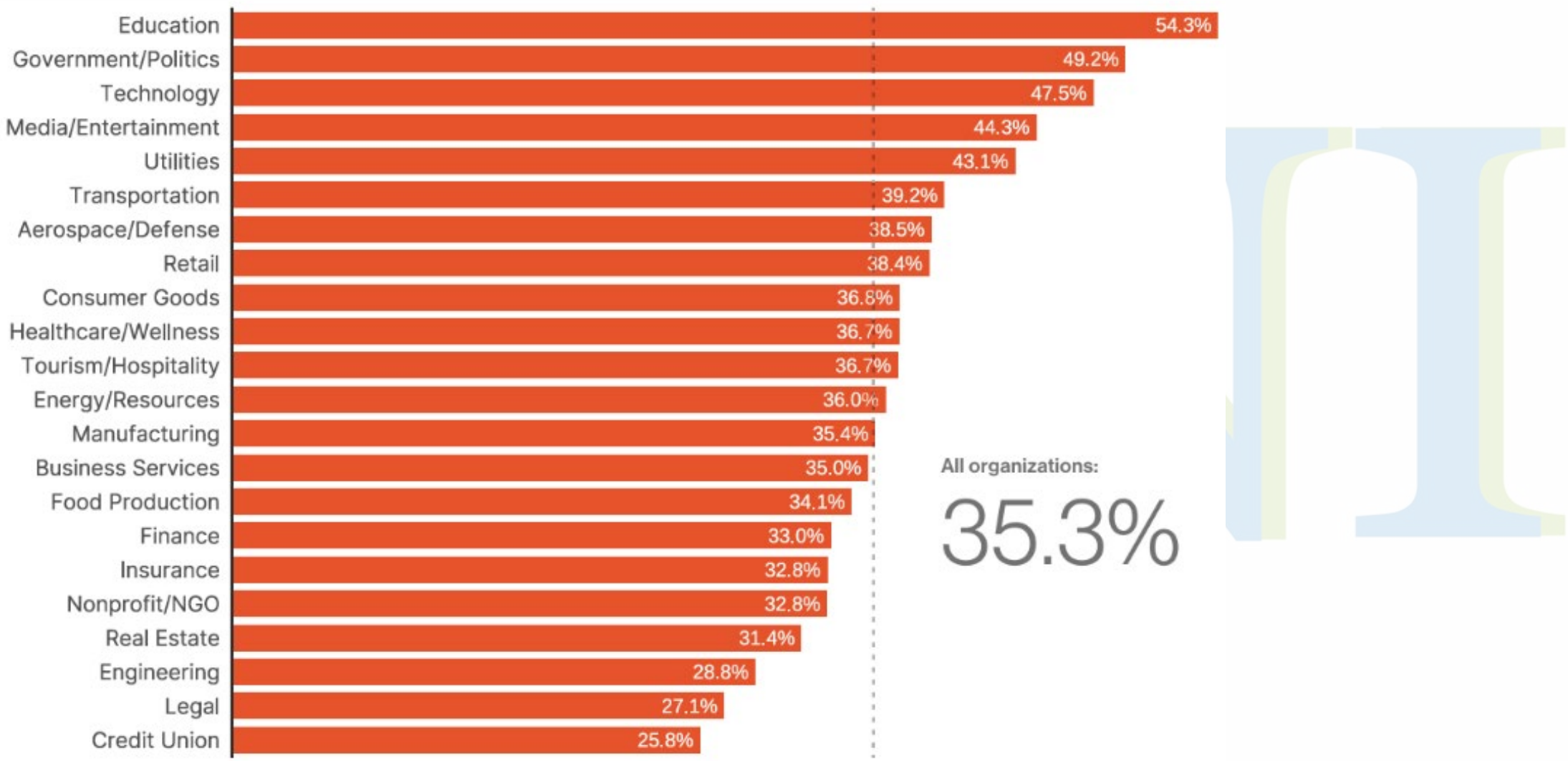
The company claimed that A.I. did most of the hacking with limited human input and said it was a rapid escalation of the technology's use in cybercrime.


By Meaghan Tobin and Cade Metz
Meaghan Tobin reported from Taipei, Taiwan, and Cade Metz from San Francisco.

Nov. 14, 2025

Louisiana Optical Network Infrastructure

Observed Incidents of Known Exploited Vulnerabilities (KEVs)



Source: bitsight.com, research from 2003-2023

For Educational Institutions…

Top 10 cyber threats:

1. Ransomware
2. Phishing and Social Engineering
3. QR Code Exploits
4. Advanced Malware
5. Distributed Denial of Service (DDoS) Attacks
6. Insider Threats
7. Third-Party and Supply Chain Vulnerabilities
8. **Cyber Espionage Targeting Research**
9. Nation-State/APT Activity
10. **Unpatched Software** and Misconfigured Systems

Strategic recommendations:

- Enhance cybersecurity infrastructure: Upgrade legacy systems and deploy modern security platforms that block malicious emails, files, and links.
- Phishing awareness and training: Educate staff and students on recognizing phishing and QR code scams. Enforce multi-factor authentication (MFA) across accounts.
- Regular system updates: Patch all systems, especially those involving communication and collaboration tools.
- Monitor and respond: **Establish proactive threat monitoring** to detect and respond to anomalies. Monitor domains for typosquatting or impersonation.
- **Collaboration and information sharing**: Partner with other institutions and threat intelligence providers to share best practices and threat data.

Source: bitsight.com

WHAT IS A SIEM? (SECURITY INFORMATION AND EVENT MANAGEMENT)

- A SIEM is software that watches over all the activity happening across an organization's computers, networks, and systems
- It gathers information from computers, networks, and applications
- It spots unusual or risky behavior.
  - The SIEM uses rules and smart analysis to look for patterns that could mean trouble
- It keeps records for investigation
  - If something does go wrong, the SIEM has a history of events—like a digital "black box"—to help figure out what happened and how to fix it.
- It helps respond quickly
  - When the SIEM finds something suspicious, it can send alerts to the right people so they can take action before problems get worse.

WHAT IS A SOC? (SECURITY OPERATIONS CENTER)

- A SOC is staffed 24x7 and uses the SIEM and other tools to help detect cyber threats
- When something suspicious is found, the SOC team immediately investigates further and takes action as needed

What a SOC *CAN* do!

- Provide 24x7 visibility into activity on your network/endpoints
  - Fill in gaps where campus resources may be lacking
- Share threat intelligence that it sees and receives
- Assist with implementing automation
- Provide information for you to make informed decisions

What a SOC *CAN'T* do!

- Guarantee protection
- Fix/patch/update/replace outdated infrastructure on campuses
- Force data to be shared from your campuses
- Force information sharing when something happens

About the SOC…

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

LONI SOC

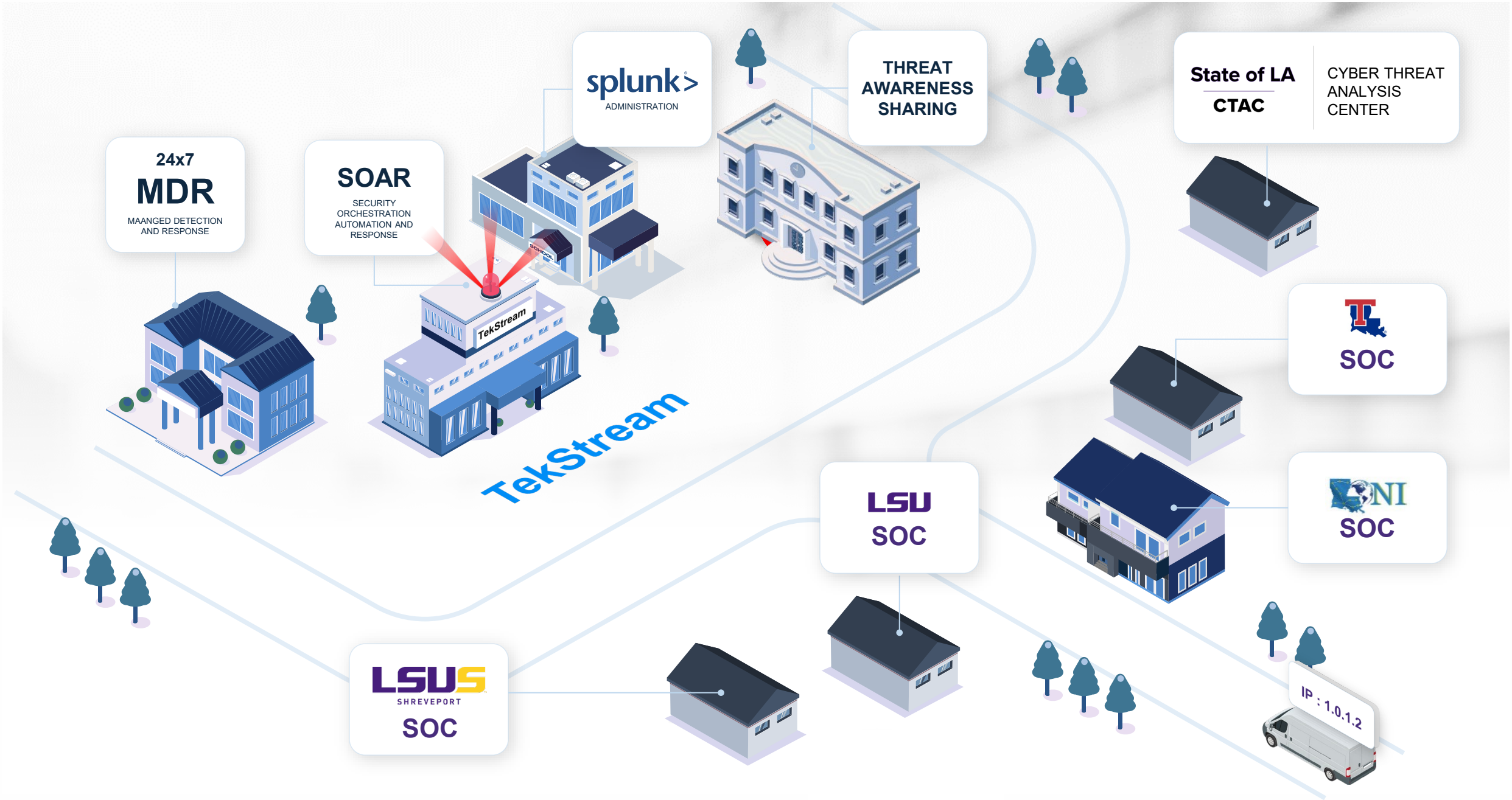

TEKSTREAM
24x7
MDR
MANAGED DETECTION
AND RESPONSE
SOAR
SECURITY ORCHESTRATION
AUTOMATION AND RESPONSE
splunk>
ADMINISTRATION
powered by
aws
School 1
School 2
School 3


LSUS
SHREVEPORT
SOC
STUDENT RUN • 8AM-5PM • MON-FRI


SOC
STUDENT RUN • 8AM-5PM • MON-FRI


NI | LSU
SOC
STUDENT RUN • 8AM-5PM • MON-FRI

32 ENTITIES

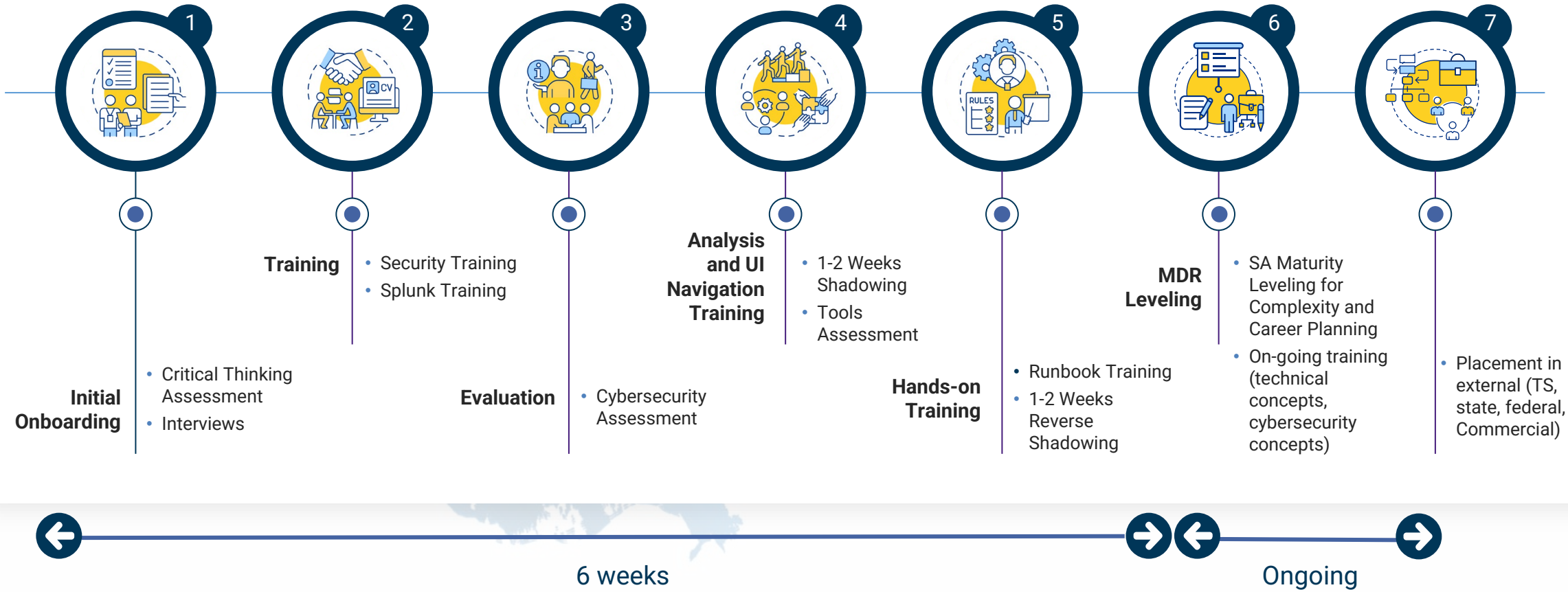


Louisiana Optical Network Infrastructure

Training Process

Student Security Analyst

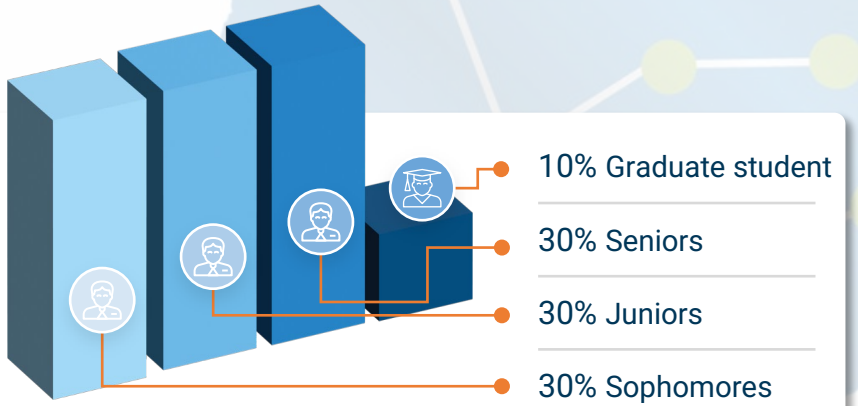
Training/Onboarding Process



STUDENT DEMOGRAPHICS

56% Male

44% Female



10% Graduate student

30% Seniors

30% Juniors

30% Sophomores

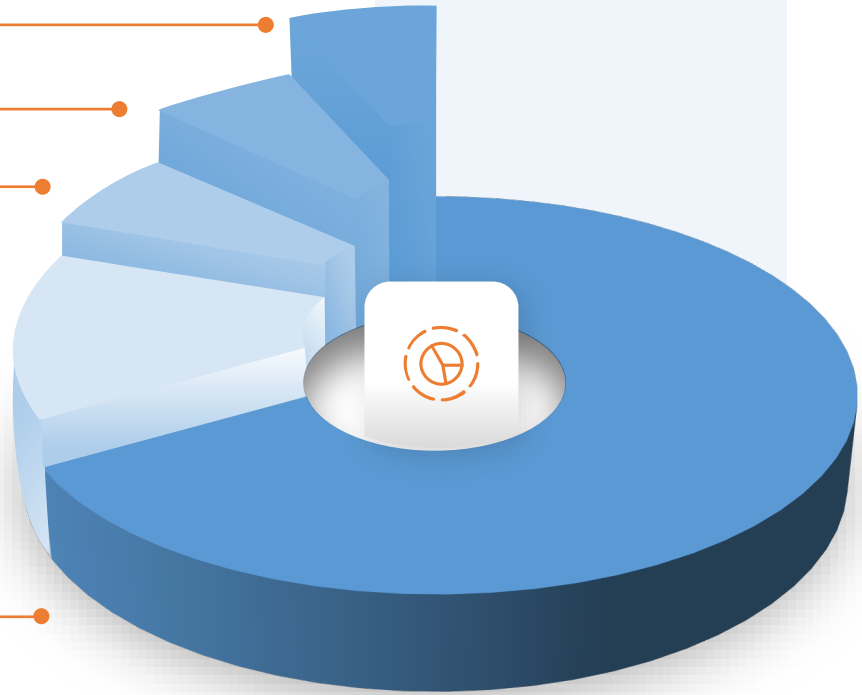
5% Psychology

5% Computer Engineering

5% Industrial Engineering

10% ISDS

75% Computer Science

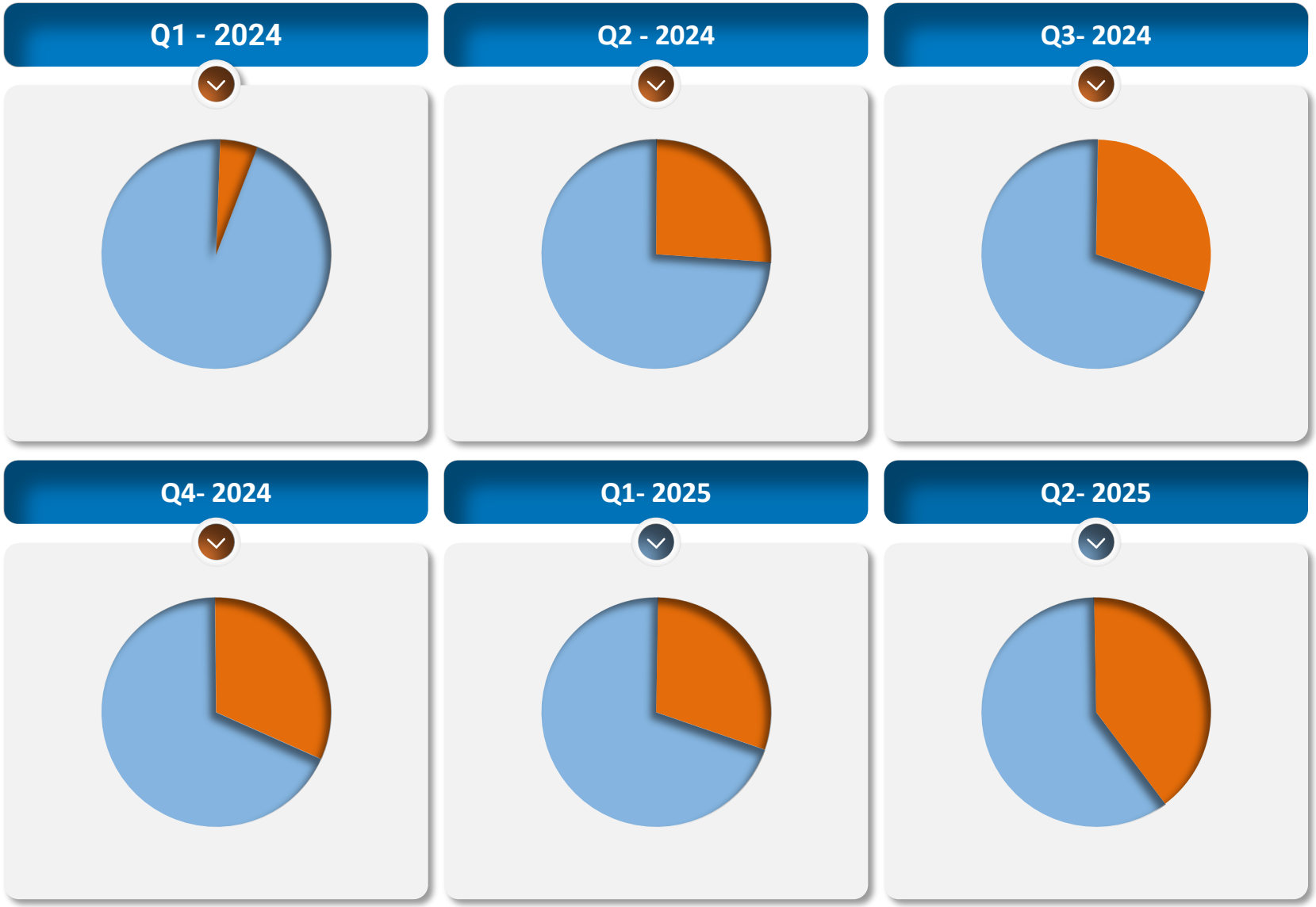


All SOCs combined, as of end of Spring 2025

Associate Security Analyst Certification

- Tailored curriculum with defined competencies per level
- Analysts follow a curated and customizable progression system
- Timeline for advancement tailored to institution and candidate pool reality
- Advancement goal to Level 3 within 2 years of entering the program
- Assessments and practicum gate advancement between levels
- Higher-level students provide tiered SOC oversight for lower-level students

Student Security Analyst Productivity Metrics



TekStream Analysts

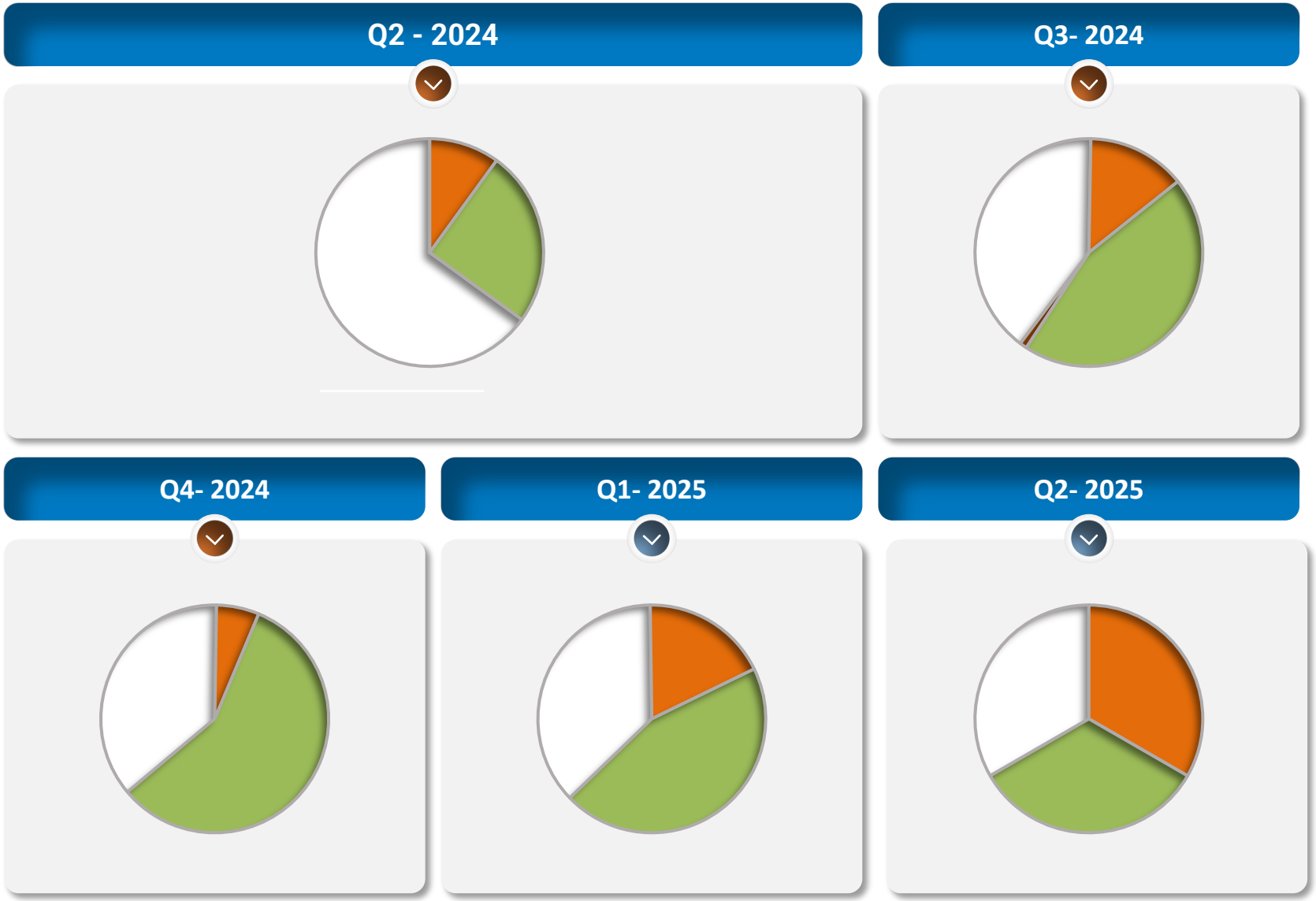
Student Analysts

Student Security Analyst Use Case Complexity Metrics

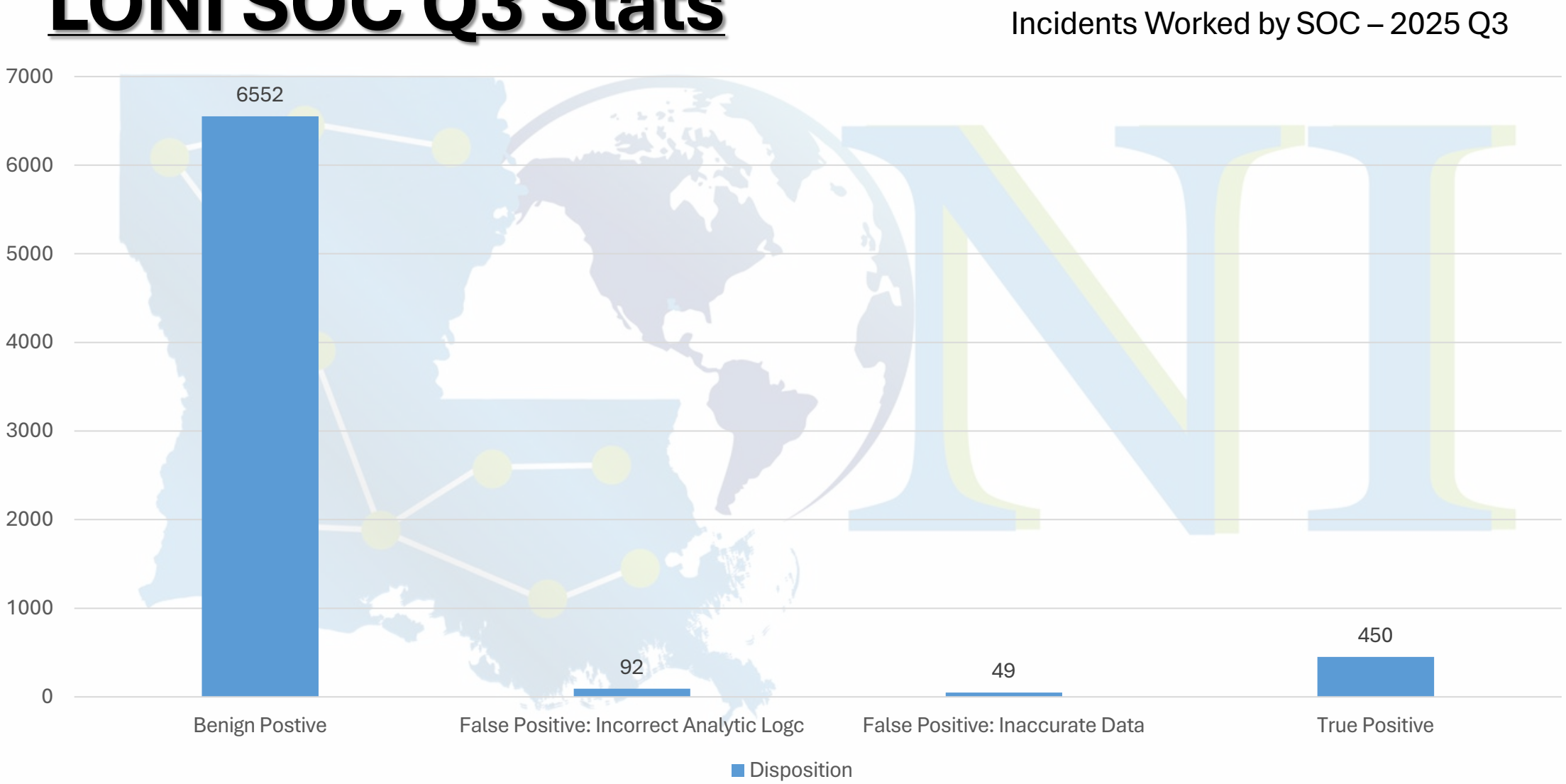
Level 1 Complexity

Level 2 Complexity

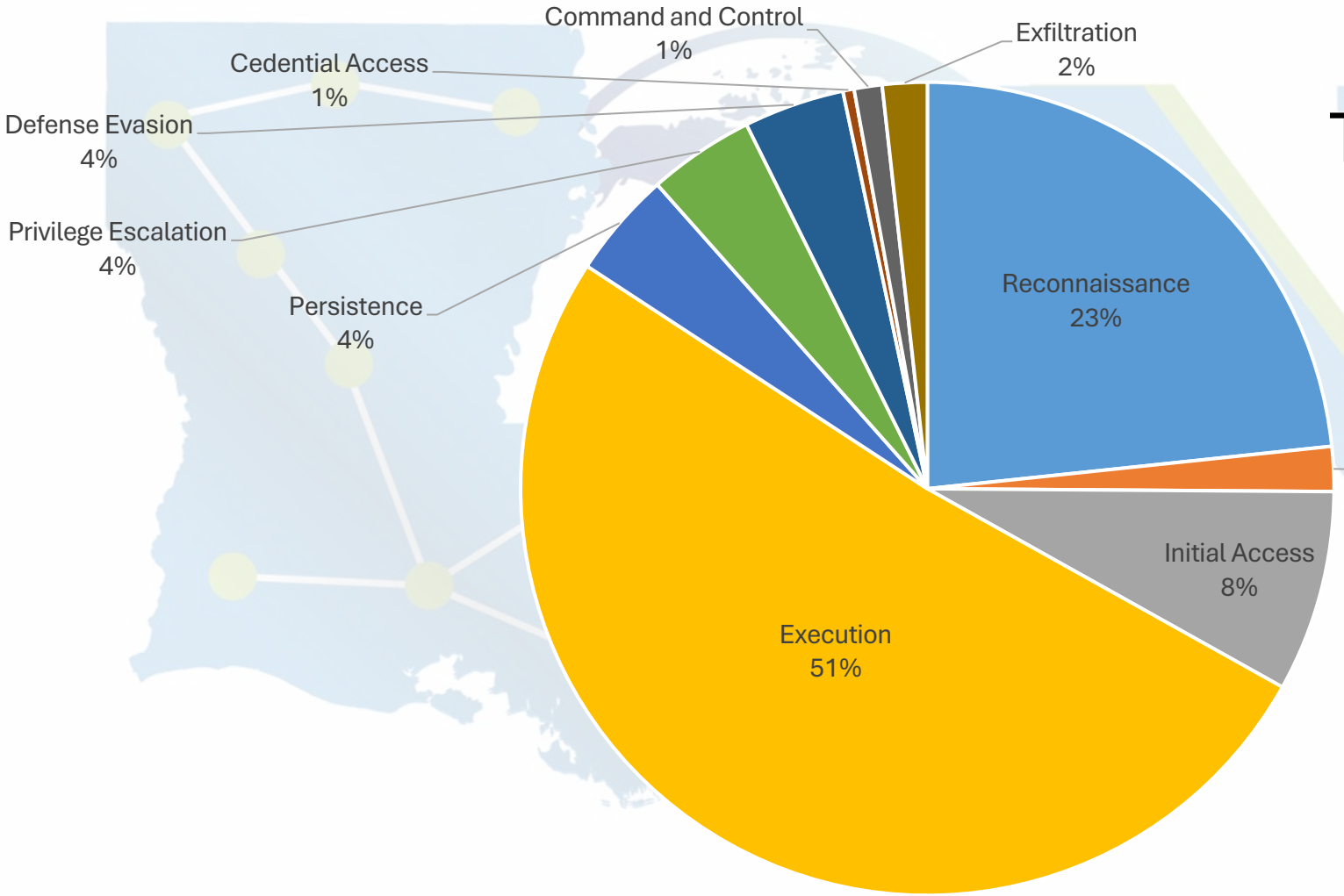
Level 3 Complexity



LONI SOC Q3 Stats



LONI SOC Q3 Stats



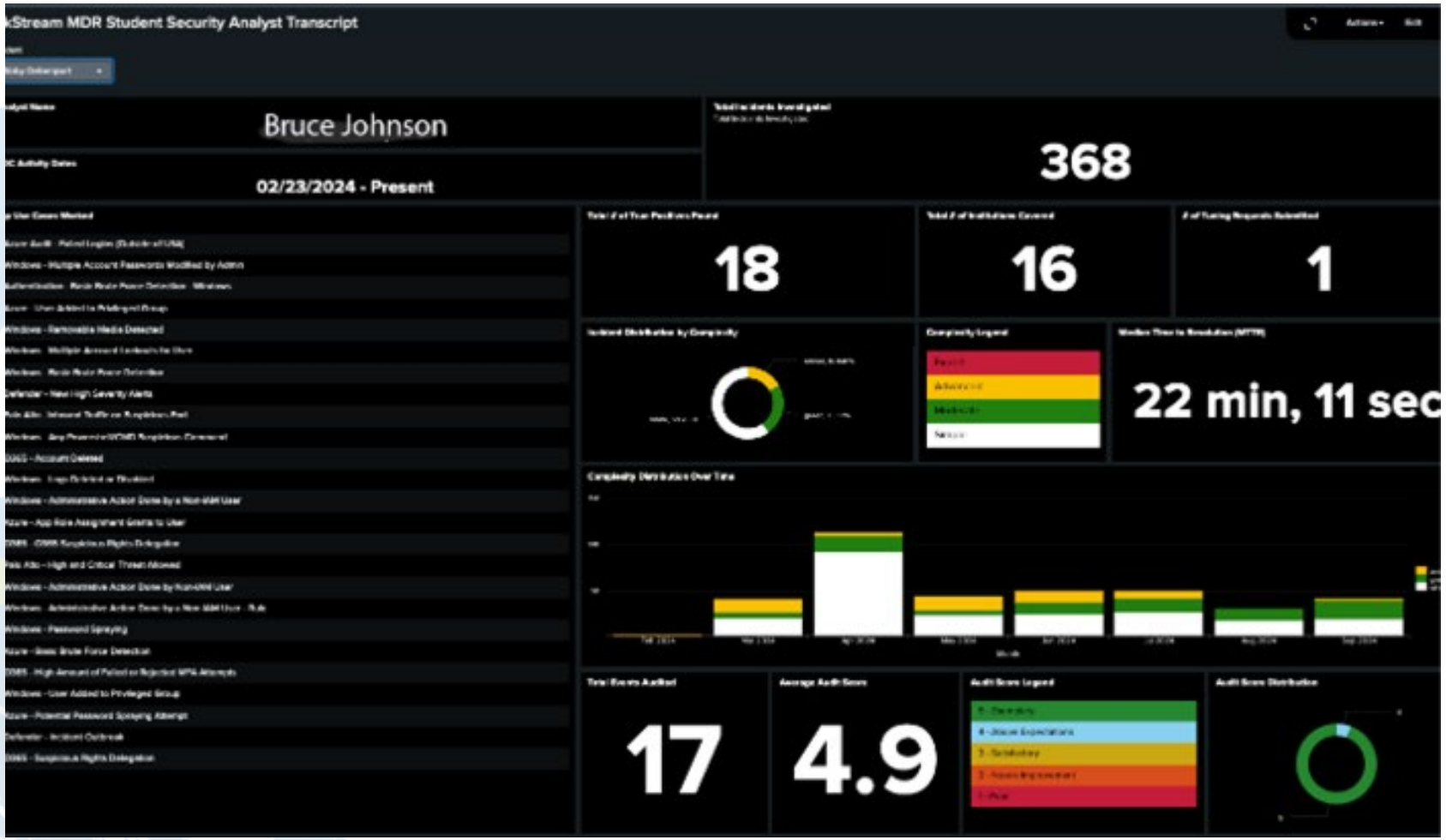
MITRE ATT&CK Technique Breakdown of True Positives

Outcomes

Student Transcript

Includes:

- Activity metrics
- Use case summary
- Complexity
- MTTR
- Scoring



Cybersecurity Career Consulting

Mentoring, Guidance, Placement

- Specialized counseling and guidance from dedicated HR & recruiting professionals
- Completion path matched to student career progression goals
- Active placement in corporate, state and federal ecosystem
- Leverages student transcript and SOC experience
- High student placement rate with more in process
- Empower student analysts to both utilize and defend against AI use cases

LSU Student SOC Analyst

Read more: Cybersecurity Career Counseling

Student Career Pathways & Placements

Graduate Placements

- Governor’s Office of Homeland Security & Emergency Preparedness
- LSU Health Sciences Center
- Epic Systems
- TekStream
- Chevron
- Proprietary Development Firms

Value-Added Benefit

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 partnered 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 eligible LONI costs.

RHC Service Funding Example 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 invoice for their allocated costs. Member institution will pay LONI thereby enabling Rural Health Care eligibility.

Contact Us

“Thank you for your partnership and for being a friend to LONI.”

www.loni.org

Follow us on LinkedIn: Louisiana Optical Network Infrastructure