GOVERNOR'S OFFICE OF HOMELAND SECURITY
GOHSEP
& EMERGENCY PREPAREDNESS

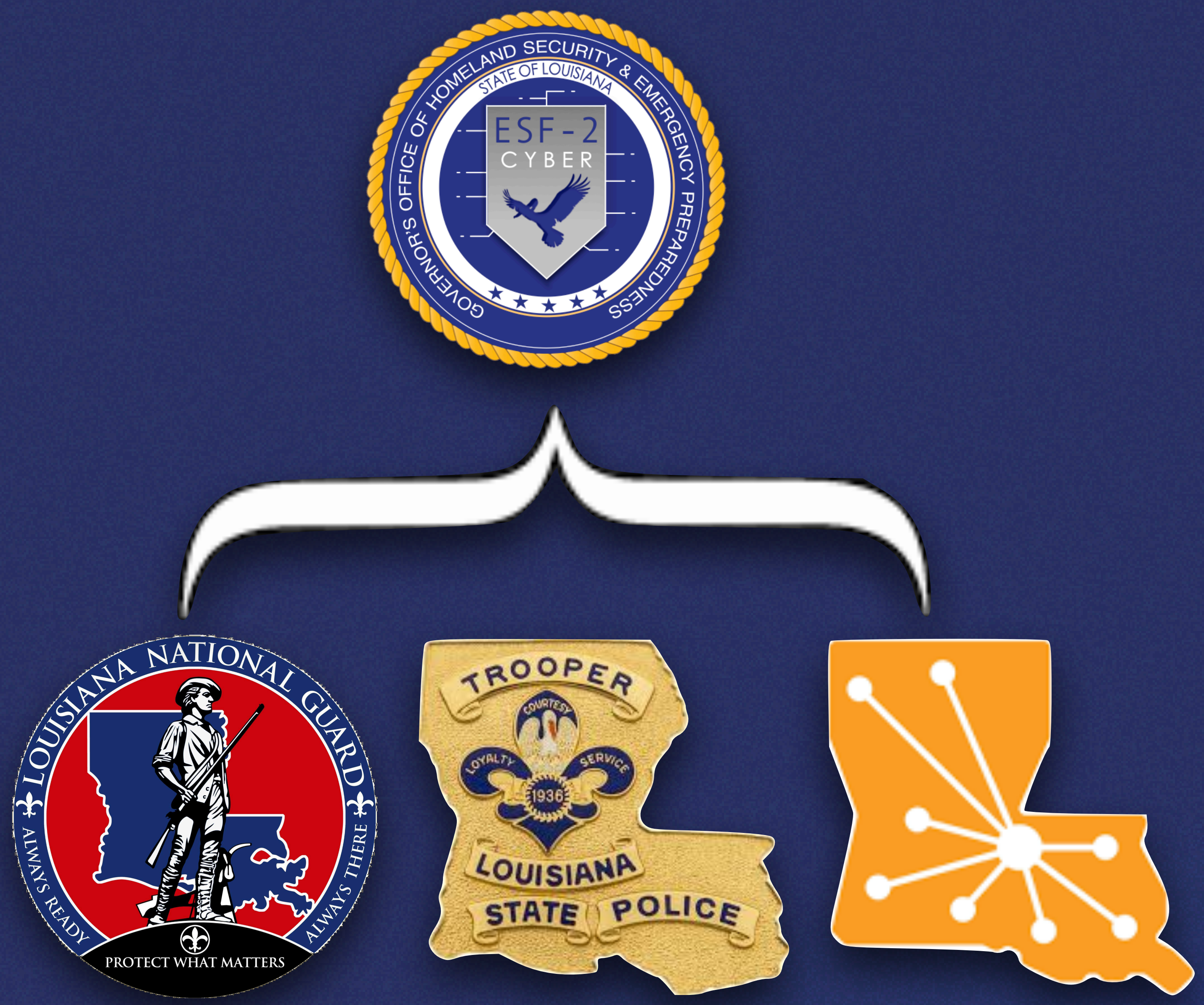
ESF-2
Cyber & Emerging Threats

Corey Bourgeois & Blake Opial

Agenda

- Who is ESF-2?
- What is ESF-2?
- ESF-2 Eligibility
- ESF-2 Benefits
- The future - Louisiana Cyber Assurance Program

Who?



- Multi-Agency Partnership

- Purpose: establish a cyber program in the State of Louisiana that can effectively prepare for, respond to, recover from, mitigate, and prevent future adverse cyber attacks. The National Response Framework Louisiana Disaster Act serves as the baseline for this endeavor.

- Formal Establishment: JBE Executive Order 19-12, which outlines the framework for conducting cyber incident response and management.

- Response Statistics:
  - 194 incident responses since 2019
  - 144,417 endpoints
  - 8,795 servers
  - All 64 parishes

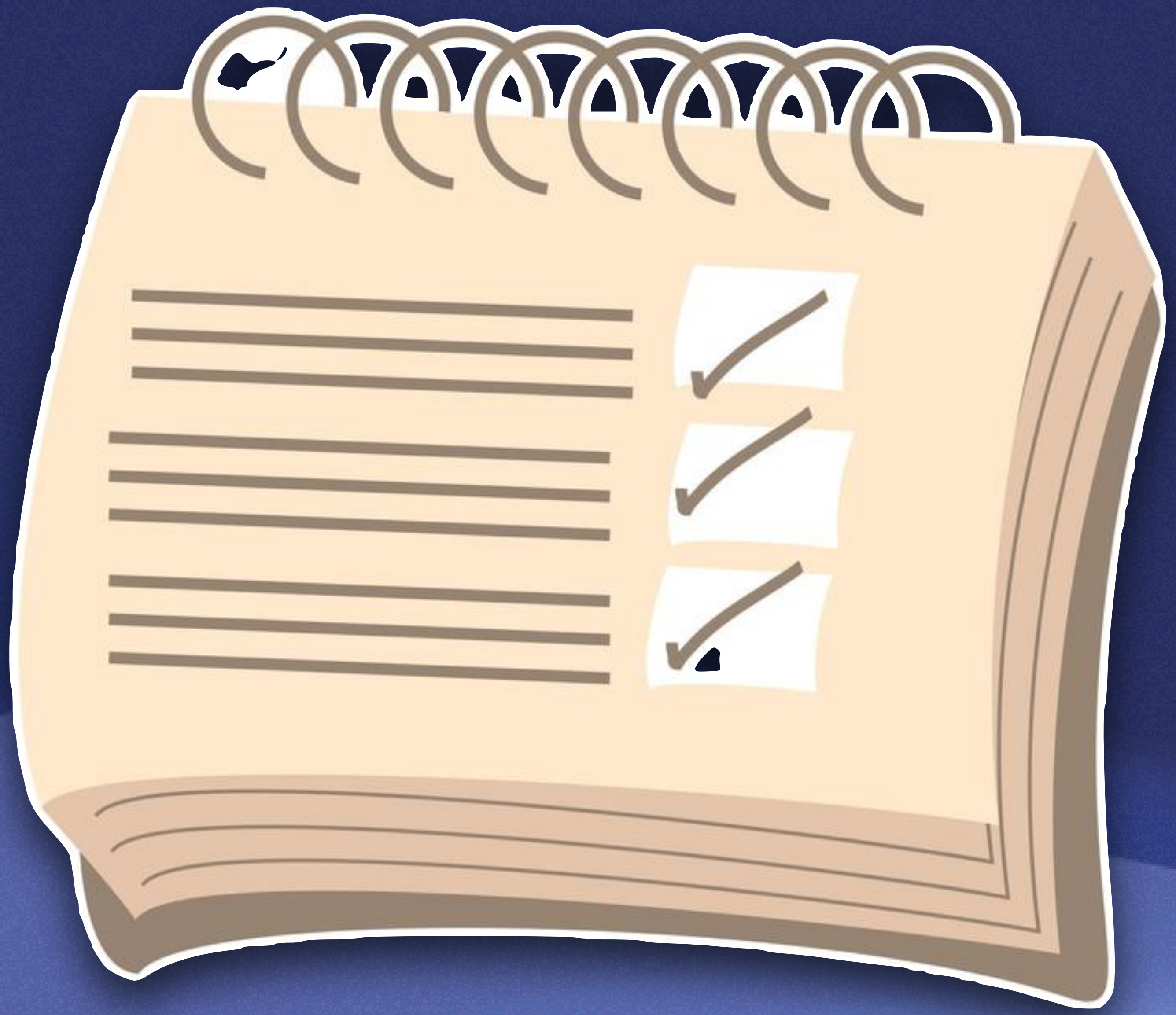
What?

- A free cyber incident response and management force composed of state employees.
- Services:
  - Digital forensic analysis
  - Cyber incident response managers that guide impacted entities through the restoration process.
  - Experienced SOC analysts
  - Subject-matter experts
  - Hardware and software for temporary use
- On-site and/or virtually support of cyber incident victim

Eligible Entities

- Qualifying Entities: State political subdivisions and critical infrastructure (GOHSEP review)
- Permissive Services: ESF-2 services are not compulsory; they are elective.
  - ESF-2 Services may be terminated at any time by victim

Requirements



- Email requesting forensic analysis to Louisiana Cyber Investigators Alliance (LCIA)
- Submission of Web EOC to GOHSEP
- Executed Memorandum of Agreement containing terms and conditions.
- Executed non-disclosure agreements for victim protection
- Adequate working conditions for ESF-2 personnel

Benefits

- No cost support
- Relationships with United States Secret Service, Federal Bureau of Investigation, and Department of Homeland Security
- ESF-2 personnel are subject matter experts
- Limited Interruption to Operations

Benefits

- Liability Mitigation: Protected by the Louisiana and Federal Cybersecurity Information Sharing Act (LA. R.S. 51:2101 et see and 6 U.S.C. 1501 et seq)
    - Provides liability protection for entities that share cyber threat indicators and defensive measures with the government and other appropriate entities. These laws shield shared information from being used for antitrust violations or to regulate the entity's lawful activities and keep the information exempt from public records requests, such as the Freedom of Information Act (FOIA).

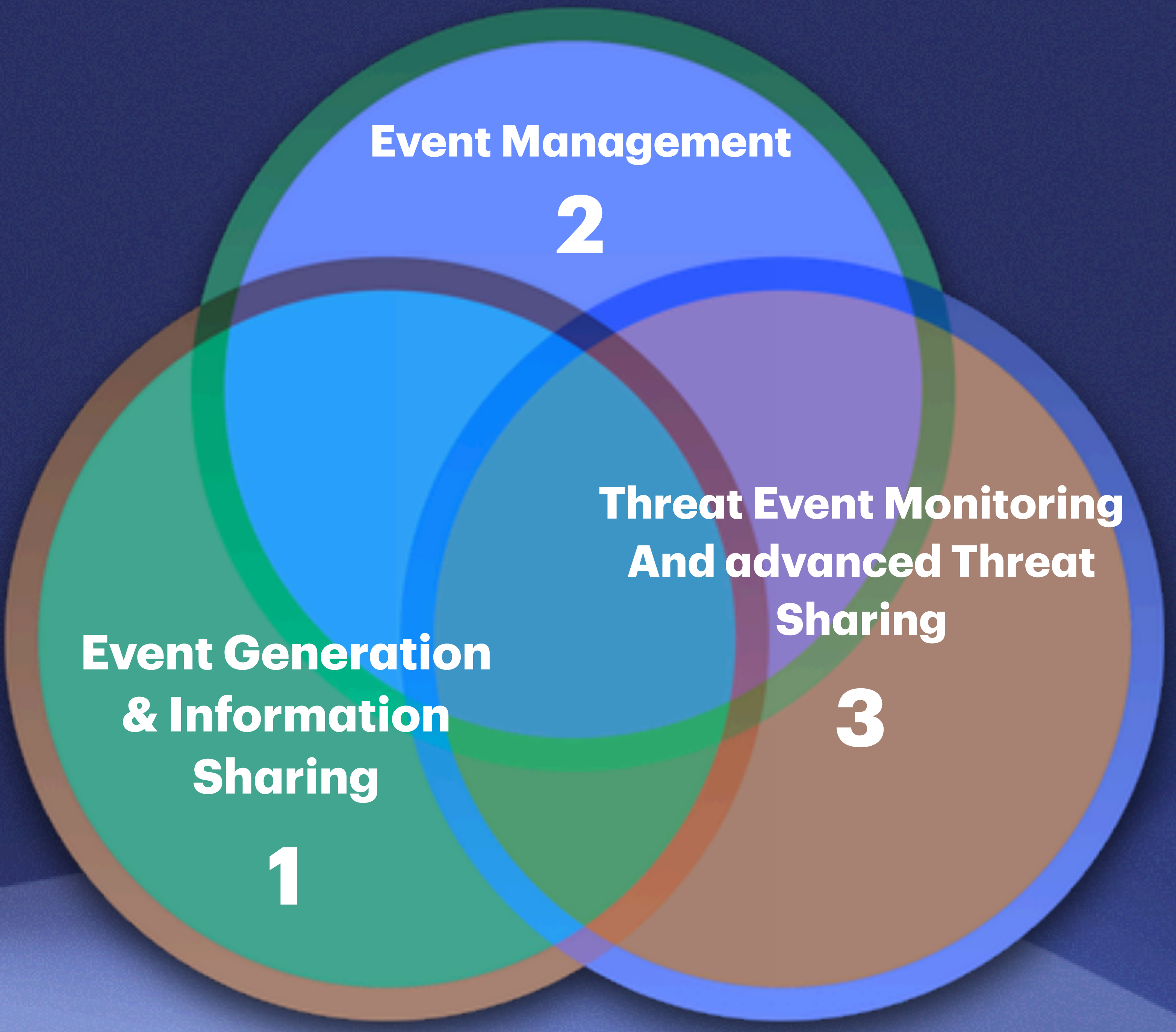
Cyber Emergency Support Function (ESF)

Objective: Formalize and establish the emergency support force for cyber.

- Using the FEMA Emergency Support Functions, States can create, authorize, and organize state commissions or task forces.
- ESF activated through the State Emergency Management Agency/ Department
- Through legislative or gubernatorial authority, give ESF specific cyber tasking consistent with State emergency response plan.
- Use steps 1-3 to nominate lead state agency(its), leadership personnel, and the agency/individual responsible for coordination with federal partners to ensure information sharing

Louisiana's Cybersecurity Future

Louisiana Cyber Assurance Program


Event Management
2
Threat Event Monitoring And advanced Threat Sharing
3
Event Generation & Information Sharing
1

- **Purpose:** Due to the success of ESF-2, this program establishes a digital ecosystem that will **collect, analyze, and distribute** cyber threat intelligence, with an active 24/7 monitored environment.
- Proof of concept was designed and tested through ESF-2 responses.
- Eligibility for LCAP Participation: Any Louisiana political subdivision no matter the size and is completely voluntary.
- Services offered:
  - Digital Forensics
  - Managed end point protection & next-gen firewalls
  - Active Threat Monitoring
  - Cyber readiness assessments
  - Incident Management

Louisiana State Police Cyber Crime Unit

- •State Police has conducted 71 cyber intrusion investigations this year
  - 56 Network Intrusions (39 Ransomware)
  - 15 Business Email Compromise
  - Continuous work with FBI, USSS, and HSI

- •Identified ~1.6 MILLION unique Indicators of Compromise (URLs, File hashes)

- Monitor, Record, and analyze 6-7 million intrusion attempts a month.
  - Largest Contributor to AlientVaultOTX with our own intelligence feed in the works

Who Do We Serve?

- Everyone
  - Citizens
  - Private Companies
  - Local, State, Critical Infrastructure, Education***

***GOHSEP rebuild availability

Rising Trends In 2025

- Malware-Free Intrusions/ Living-Off-the-Land (LOL) Binaries
- Reverse Shells
- SEO Poisoning
- AI “Copy Paste” Data Exfiltration
- Vishing/Deep Fakes
- Faster Encryption (1 week to 48 hours from exploit to Encryption)

Common Issues

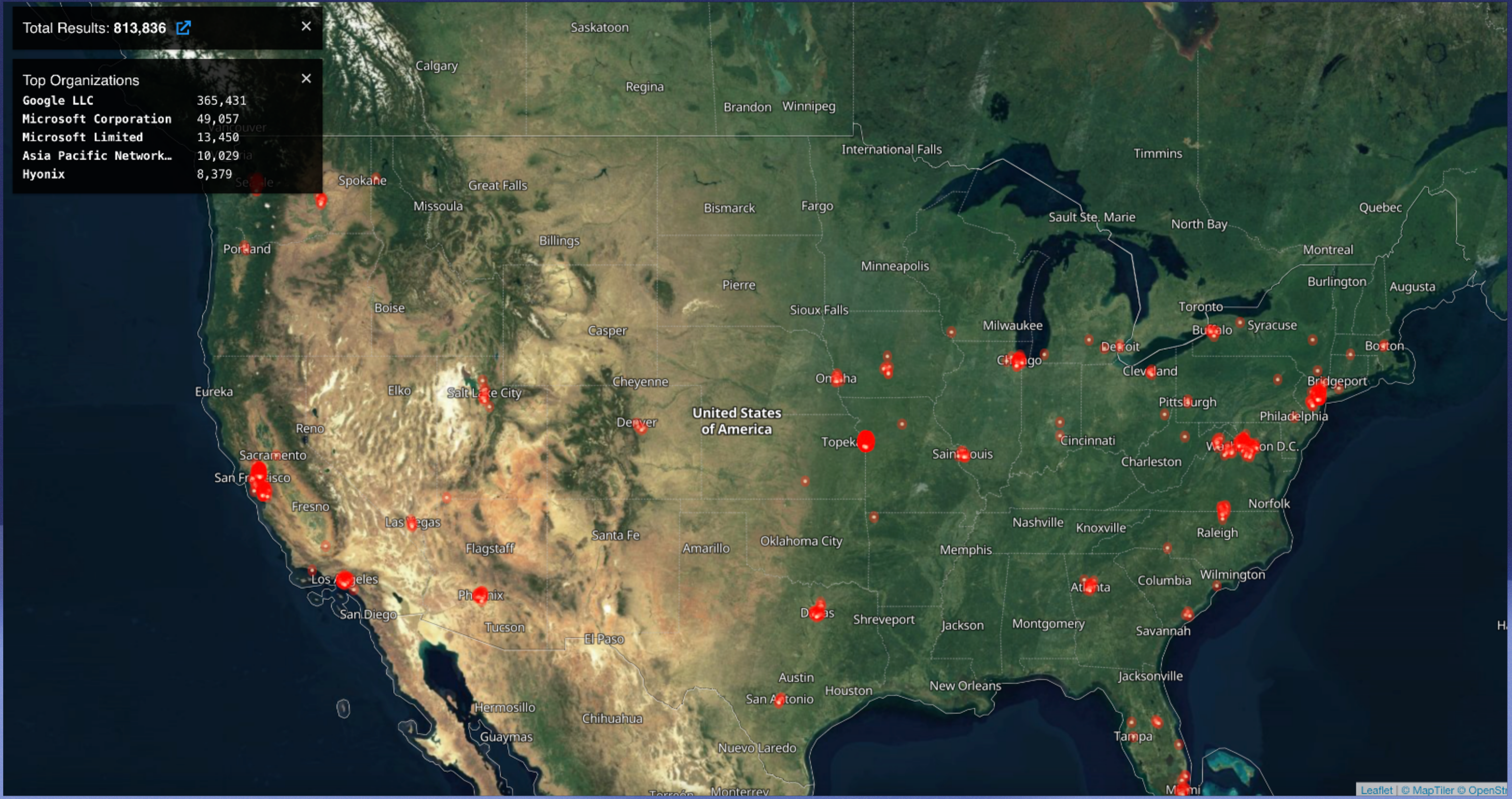
The following technical configurations significantly contribute to creating vulnerable environments:

- All users were granted administrative privileges on workstations.
- Basic network segmentation was not applied.
- Backups were not stored off site or offline.
- Updates were not applied consistently.
- Exposed Remote Desktop Protocol.
- No Centralized Logging.
- Minimum Password Requirements.
- Zero MFA implemented.

GOVERNOR'S OFFICE OF HOMELAND SECURITY
GOHSEP
& EMERGENCY PREPAREDNESS

Open RDP

Taken: 11-18-25



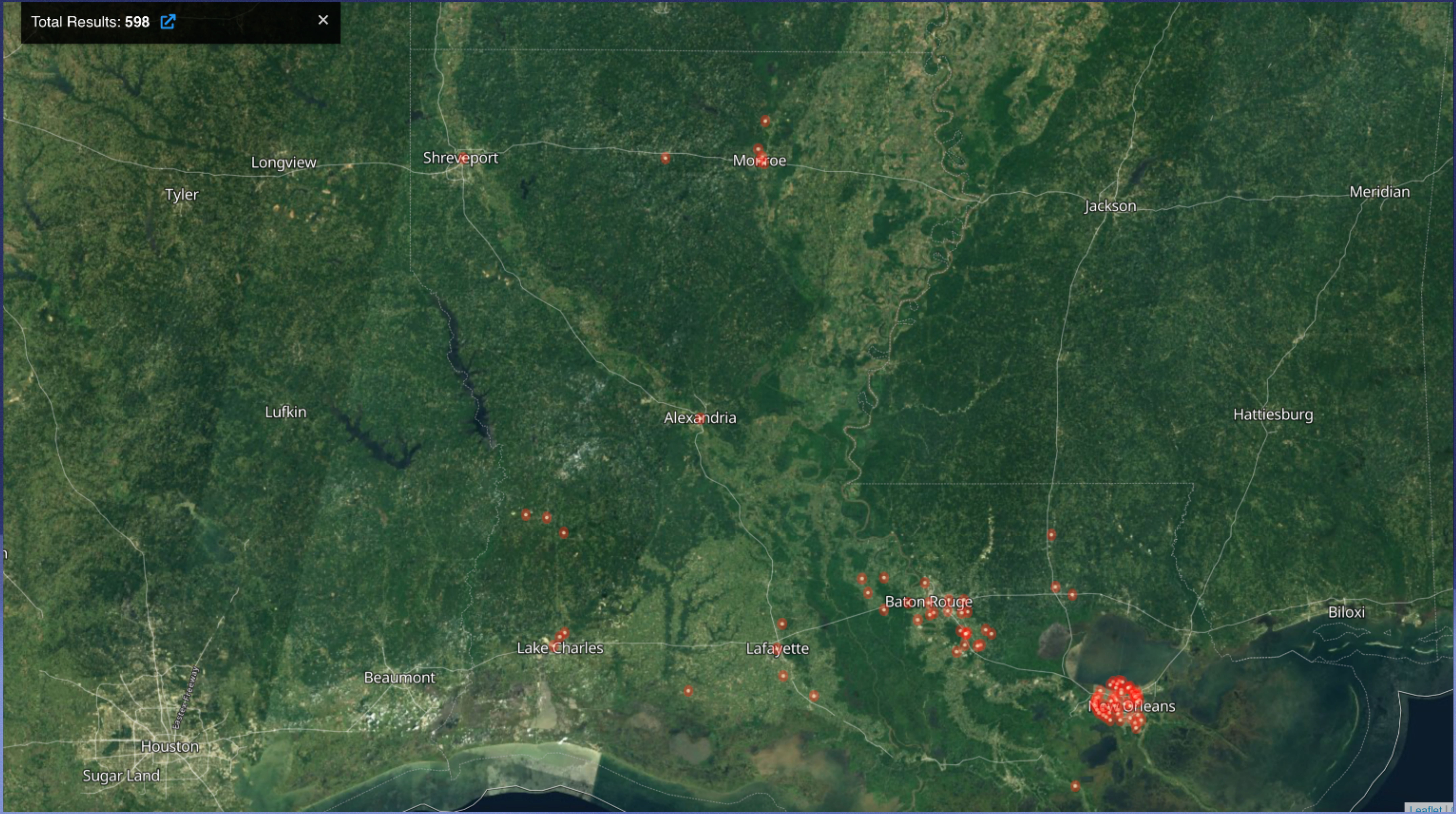
Total Results: **813,836**

Top Organizations

Google LLC	365,431
Microsoft Corporation	49,057
Microsoft Limited	13,450
Asia Pacific Network…	10,029
Hyonix	8,379

Open SMB

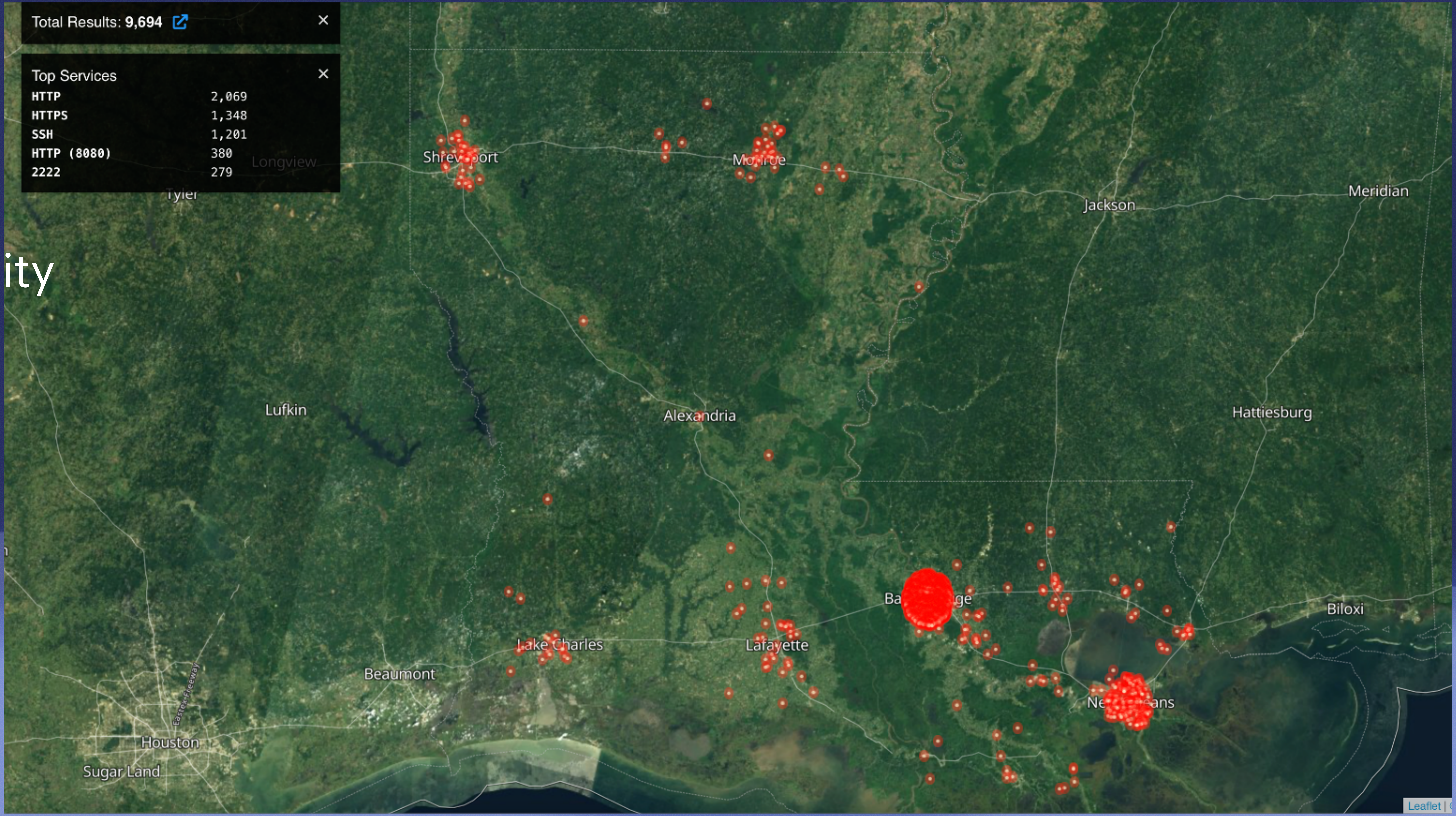
Taken: 11-18-25



Total Results: **598**

Vulnerability

Taken:
11-18-25



Total Results: **9,694**

```
Top Services
HTTP               2,069
HTTPS              1,348
SSH                1,201
HTTP (8080)          380
2222                 279
```

Expectations From Law Enforcement

- Should be able to collect evidence without taking hardware
- Activity should minimally impact operations, Remotely if possible
- Often work with outside IR Teams/Cyber Insurance Companies and provide findings
- Should provide a complete report of findings to include:
  - Most probable vector in
  - Patient Zero
  - Indicators of Compromise

Evidence Collection Process

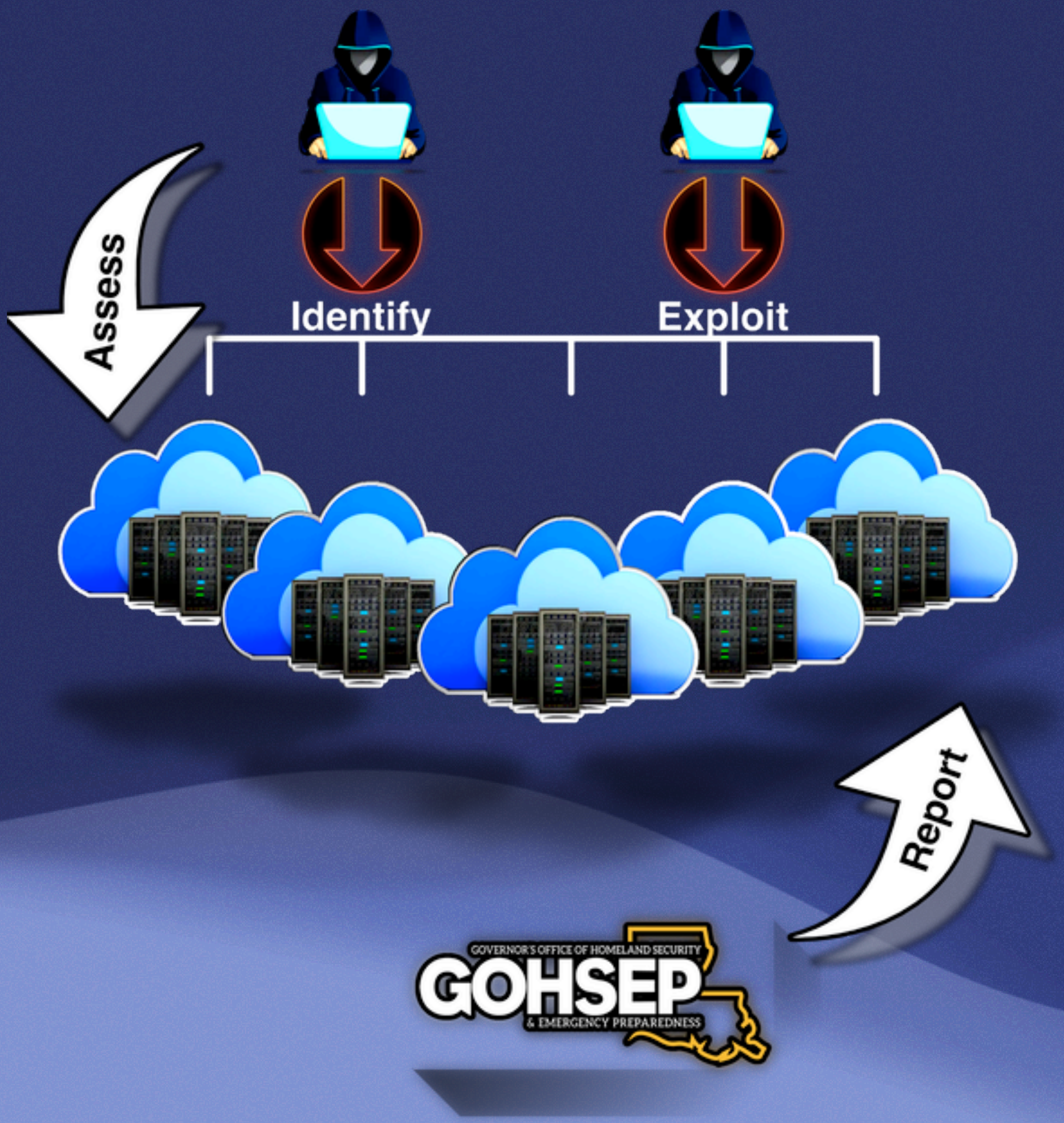
Order of Volatility ("What to grab first")

1. Memory
2. Routing Table, ARP Cache, Process Table, Kernel Statistics, Active Connections
3. Temporary File Systems, Event Logs, and Application Logs
4. Disk
5. Remote Logging and Monitoring Data
6. Physical Configuration and Network Topology
7. Archival Media

**All collections performed with industry standard tools and procedures

Incident Response

Office of Cyber Readiness



- Goal: for OCR to assess Vulnerabilities and report findings faster than the attackers
- A division of Louisiana's Cyber Assurance Program within LA GOHSEP
  - Services Include:
    - Vulnerability assessments
    - Documenting results
    - Recommendation on improvement/changes
    - Consistently verifying and validating improved cyber posture
- Was implanted in December of 2022
- Have conducted and delivered over 200 assessments to date

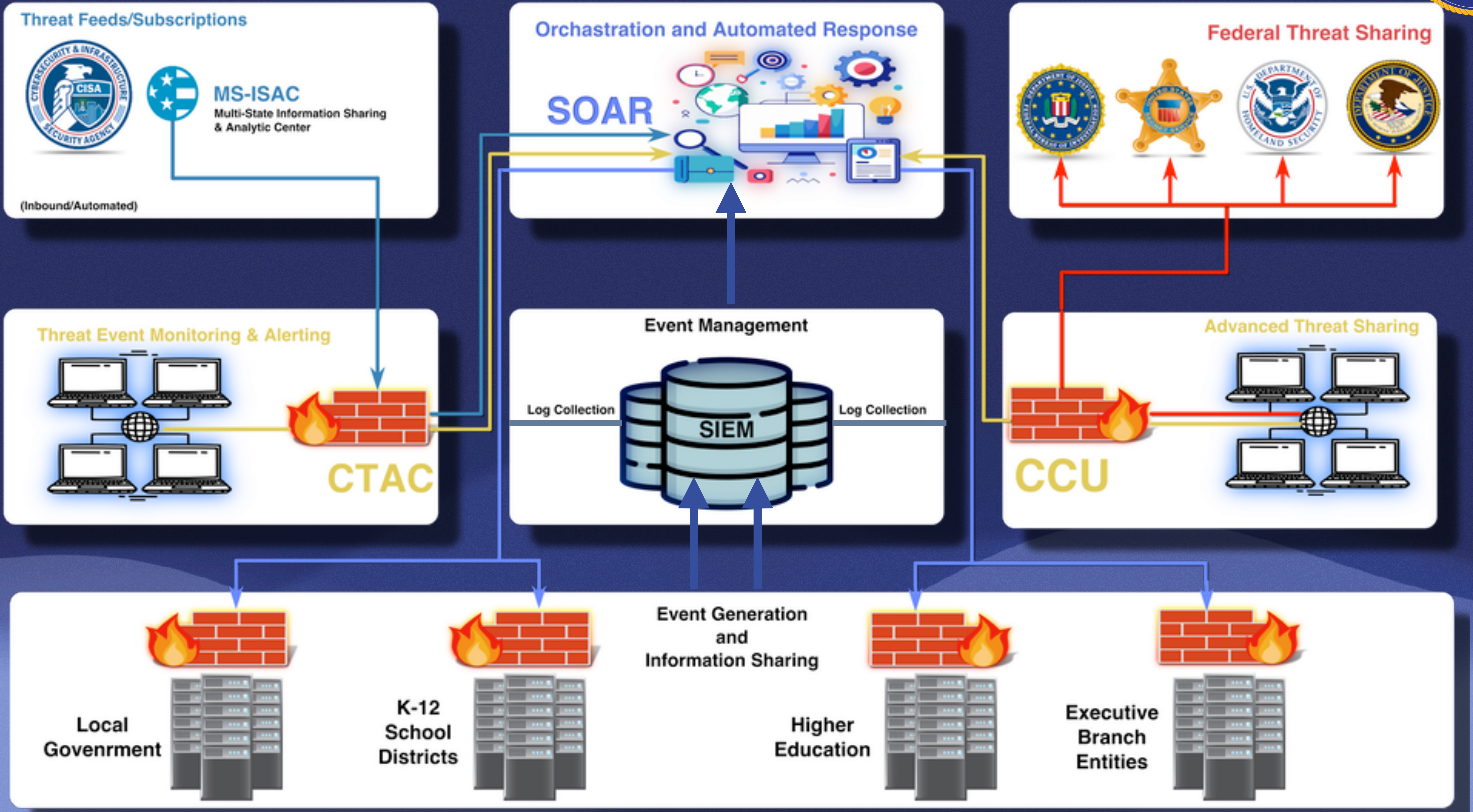
Cyber Threat Analytic Center

- Another division under the Louisiana Cyber Assurance Program

- CTAC conducts advanced active threat monitoring and information sharing.

- Uses multiple collection tools
  - Captures event logs
  - Sends to SOAR
  - Automatically pushes defensive commands to protect networks
  - Was implemented in 2024

GOVERNOR'S OFFICE OF HOMELAND SECURITY
GOHSEP
& EMERGENCY PREPAREDNESS



Threat Feeds/Subscriptions

MS-ISAC
Multi-State Information Sharing
& Analytic Center

(Inbound/Automated)

Orchastration and Automated Response

SOAR

Federal Threat Sharing

Threat Event Monitoring & Alerting

CTAC

Event Management

Log Collection

SIEM

Log Collection

Advanced Threat Sharing

CCU

Event Generation
and
Information Sharing

Local
Govenrment

K-12
School
Districts

Higher
Education

Executive
Branch
Entities

Balancing Reactive With Preventive

- ESF 2 Metrics
  - Constant activation since 2019
  - 133,281 sensors deployed
  - 194 Incident Responses
- Shift Focus to Prevention
  - GOHSEP, LANG, and LSP have designed and formalized the “Louisiana Cyber Assurance Program” which will drastically improve the State’s preventative cybersecurity posture.
  - Will Maintain proper monitoring of the assets previously deployed by ESF-2 to assist local government entities with on-going threat mitigation.

?

CCU Contact:
lcia@la.gov

To Report a Cyber Crime:
Lafusion.Center@la.gov